**EMCS2200: Global Cyber Challenges: Law, Policy, and Governance**

Post-Work: Briefing Paper  
Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

*The bipartisan select committee has held several hearings and staff are beginning to draft an interim report with recommendations for action. Draft a 700-word paper with agenda items that could serve as an executive summary for the report. This document should include several recommendations to address the cybersecurity challenges you emphasized in your pre-work assignment and discussed during the residential session.*

**Growing Number of Highly Coordinated Sophisticated Attacks**

There are several indications that the level of sophistication of Threat Actors in growing. Private Industry, Government Agencies, and even Non-Profit Forums have all reported many different separate and distinct Advanced Persistent Threats ( APTs ). These threat actors have moved beyond simple Malware Injection/Scripting and/or Command-Control techniques. Instead, they are combining many different techniques, sometimes even setting up fake corporations and hiring unwitting US citizens to commit crimes. To counter these efforts we need unified training for Government Employees, Coordination with Private Industry around threat reporting and to agree on policy as a response to Threat Actors according to their activity. As we enter a future where ongoing cyberwar, clandestine sabotage, and cybercrime are the preferred venues for bad actors, we need to train our users, coordinate across sectors and find agreement where we can as it pertains laws that govern technology.

**Need for Unified Comprehensive Training**

While there are some departments and agencies that provide CyberSecurity training for their Employees and Contractors, the training is not always complete, up-to-date or engaging. Users in any system are the weakest link and often “lower the drawbridge of the castle” by accident. Creating CyberSecurity training is no easy task, but it’s a challenge worth the hard work. A well informed and vigilant user is worth much more than the strongest firewall. Training users how to create ( and remember ) strong passwords, protect PII, spot and report suspicious activity and avoid phishing attacks should priority one for every department and agency in the government. Unifying the training into on central course, with sub-courses for specific departments and agencies will ensure the material’s accuracy and relevancy.

**Need for Coordination with Private Industry**

Attackers often don’t care who is in the line of attack if the target information is valuable. Government secrets in the custody of a contractor or PII on the care of the government have the same value on the black market or in the hands of foreign intelligence. A joint commission on CyberSecurity that meets on a regular basis, includes a real-time forum for the exchange of ideas and threat information, and works together to form policy, provides the necessary brain share needed to create the layered defense we need to counter the myriad of threats that surface each day. This joint commission should consist of individuals with security clearances, organized by industry and technical expertise along with program managers who mediate ideas across disciplines.

**Need for Policy**

We can all agree that there is a void when it comes to policy, as it relates to CyberSecurity. Creating laws can be challenging due to the quickly evolving landscape, partisan posturing and the changing of the guard every 4 or 8 years. However, even in the face of these challenges, there are a couple mandates we can all agree on.

People who break the law will be indicted ( at the very least ) not matter where they are. The power of indicting people who break the law even if they are outside of the US is underrated. Individuals who break into our systems ***should*** be fearful that they will be prosecuted, in the same way, criminals are prosecuted here in the US. This doesn’t mean we scrap due process, but hackers who break the law abroad should think they are Scott Free because they live in countries where these types of crimes are condoned. At the very least they will be on an Interpol list.

Operating Systems and Enterprise Software must meet a Federal Security Standard. Much like the FDA and USDA dictate a standard for food, we should have a standard for software. We trust the FDA, EPA, USDA and other agencies to keep the foods we eat safe, the air we breathe clean and drugs we use compliant. Software that runs our infrastructure, our financial systems and our communication systems should be held to a high standard, one created by our best experts. In congruence with the requirements mentioned above, providers who want to offer software for sale to more than 1000 people in protected sectors should be required to meet a standard for security. This may be controversial, but considering what is at stake, I feel it is a necessary step.