Santee Cooper's Response to CIDAWG White Papers

1. **Prospective benefits of a trusted data repository (6/2015)**

   This paper lays out the key goals of developing a repository of data on cyber-attacks. It claims that the market for cyber coverage is being stymied by a lack of credible actuarial data with which to underwrite the risk and differentiate exposure. The philosophy driving this aspect of the repository is that the free market mechanism of insurance premiums can play a key role in driving prudent investment in proven preventive measures. Given an array of current loss data, insurers would be able to identify underwriting criteria to allow differentiated pricing according to perceived vulnerability. Their customers, responding to high premiums, will invest in preventive procedures and technologies in order to lower the cost of insurance (or perhaps even simply to qualify as "insurable"). Of course, the data would also be available to trusted information security officers who could also employ it to ensure their organizations remain on the cutting edge of best practices for loss prevention and mitigation. Several value propositions were shared including: 1) identification of effective controls 2) informing peer to peer benchmarking 3) identify financial return for various security and other investments 4) identifying industry sector, regional and seasonal trends 5) supporting forecasting and modeling and 6) supporting the evolution of a cyber risk management culture.

   Potential shortcomings:

   - The implication of a repository making insurance cheaper and more universally available is flawed based upon current information. The market for cyber-risk insurance if flooded with capacity at competitive rates. The market forces of opportunity and competition have created broad coverage forms at low prices as early adapters seek to build market position. Better information will ironically likely tighten underwriting standards and raise prices – at least in the short run.
   - Some insurers have invested in the development of their own databases which they view as a competitive advantage. It will be difficult to convince them to share this data with a broader group.
   - With the nuclear industry as backdrop, I worry about the development of an "arms race" as organizations vie to stay ahead of continually evolving best practices. The phenomenon known as "ratcheting" in the nuclear field conveys a situation where an incremental improvement – no matter how insignificant – must be replicated by all industry members.

- The repository is a classic example of a "public good" in economic terms. The challenge will be to incentivize participation in data collection and determine how best to fund this project.

2. **Consensus data categories for a data repository (9/2015)**
   This paper evaluated the types of data which might be collected in a centralized repository, balancing the advantages of comprehensive data against the need to keep reporting simple and thereby encourage participation.

   Potential issues:

   - The self-reporting of post loss data presents potential challenges to accuracy. It will be difficult for an organization that has just experienced a loss to admit that its defense posture was weak immediately prior to the attack. There might also be competitive disadvantage perceived in revealing the financial impact of a loss.
   - There is some fear that reporting data after a loss might be resisted if an entity is in the midst of a coverage dispute with its cyber insurer.
   - There is the potential for duplication of effort when measuring these recommendations against the requirements of the Cyber Security Act of 2015 and other regulatory acts that require reporting. It is posited that simply adding a category of "financial impact" to existing reporting requirements would round out the data required to more efficiently underwrite this exposure.
   - Some of the categories are subjective – such as "What was the apparent goal of the hacker"? Also, the amount of data proposed to be reported is perhaps broader than would make reporting an easy process. As valuable as the repository might be, there will be insufficient data provided if the developers do not take pains to keep it simple.
   - For a variety of reasons, the group has made it clear that it would be counterproductive for the government to run this proposed repository. This begs the question who will manage it and how will they be compensated. We understand there are private firms currently bidding to manage the repository.

3. **Overcoming perceived obstacles to the establishment of a repository (12/2015)**
   This paper both identified and challenged postulated objections to the creation of a standardized repository. Among the most significant concerns are those related to the confidential nature of data supplied, and the prospect that the repository itself could be the subject of a cyber-attack. It was also pointed out that some types of attacks might

be so unique as to make it impossible to report with assurance of confidentiality. Some insurers believe participation could impair their ability to contest a claim. Finally, there is concern that the sharing of data might in some manner expose data providers to legal liability.

Potential Issues:

- It is safe to assume that a group skilled enough to be selected to manage a repository could also do so with appropriate confidentiality and anonymity. The document offers a number of methods to ensure this. The challenge is that they inevitably drives up the cost of the operation and complicates data entry, submission, and employment of the database.
- The repository is proposed to incorporate the data of U.S. companies only in its initial phase due to varying privacy laws and cultural issues with non-U.S. owned companies. Certainly understandable, but will leave a void in data and impose a cost on U.S. companies that their competitors may not have to bear.
- It is likely that access to the data repository will only be provided to active participants in the concept. This may be the only way to foster participation. This presents issues as well, since organizations that have not suffered a breach may receive a "free ride" to data access as they will only be required to pay the fare (data contribution) once they experience a loss.

Conclusion – There is little doubt that the type of repository contemplated by the CIDAWG can help society better manage this emerging risk exposure. Like many things in life, the real devil is in the details, as has been demonstrated in spades by the work of the CIDAWG. These volunteers have made great strides in identifying issues related to the proposed repository, but much work remains to be done.