CEP Magazine - June 2022
Cyber risks: How are you measuring and mitigating them?

By Teri Quimby, JD, LLM

Teri Quimby (teri@teriquimby.com) is an attorney, speaker, author, consultant, and former state regulator in Lansing, Michigan, USA.

- linkedin.com/in/teriquimby


Teri Quimby

Picture this: The workday starts out like most other days and inevitably involves electronic devices for many of us. Our expectation, realistic or not, is that technology will work at our command on a 24/7/365 basis. Then—a system disruption occurs from an external source. The focus of the day forcibly shifts. Are conversations centered around in-place preventive practices protecting information? Or around reactionary measures now tossed about like lifeboat attempts to save information where possible?

Public and private collaboration

Cyberspace security challenges in the US are well documented for the private and public sectors. These concerns have the attention of many federal agencies and entities. The work of the U.S. Cyberspace Solarium Commission, for example, concluded that coordinated action plans are needed across many fronts. Established through federal legislation in 2018, the Cyberspace Solarium Commission issues annual updates with the most recent being the *2021 Annual Report on Implementation*.[1] It doesn't sugarcoat the viewpoint that it is time for leaders in business to step up and accept responsibility: Proactive protection measures are overdue for critical infrastructure and information. Government must also do the same to address its own impediments, where "issues of jurisdiction, bureaucracy, and underinvestment hamper efforts to combat cyber threats, build effective public-private collaboration, and promote responsible behavior in cyberspace." To accomplish this, the commission formulated 82 initial recommendations, supplemented by white papers. While many recommendations require legislative or executive action, the commission highlights those that have already been successfully implemented. As recommended, the new position of national cyber director was created; it has been filled by Chris Inglis.

Director Inglis is a well-publicized proponent for collaboration between government and industry, who categorizes it as a vital partnership and key to data privacy. This collaboration is viewed as movement in the right direction to prevent cyberattacks in the first place, and to assist with countering and recovering from them. The level of risk involved is viewed as a burden to be shared and addressed through public–private collaboration.[2] Also, to foster these public–private sector relationships to manage and drive down risks prior to incidents, the Cybersecurity & Infrastructure Security Agency established the Joint Cyber Defense Collaborative in August 2021.[3] More and more government resources are becoming available for collaborative efforts with the private sector.