Towards a Collaborative Effort to Unlock the Cyber Insurance Potential

Chris Finan

The Obama administration issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February, 2013, after the US Congress failed to pass comprehensive cybersecurity legislation. Among other provisions, the order directed the National Institute of Standards and Technology (NIST) to generate a framework of standards and best practices for cybersecurity risk reduction, the strategic intent of which was to create a common commercial risk assessment methodology. The administration reasoned that a common cyber risk framework would help improve actuarial modeling and enable additional insurance offerings. The NIST framework has been widely adopted and is contributing to the growth of the cyber insurance industry. Nonetheless, cyber risks continue to persist and have yet to be sufficiently understood or addressed by many organizations, with consumers and citizens likely to bear much of the cost of the resultant harms.

As state-sponsored cyber attack capabilities proliferate, the risks become more difficult to mitigate and industry is rightly questioning whether the responsibility for defending against state-based actions should fall on the private sector. This debate raises additional questions around moral hazards from direct government intervention and the need for more direct regulation to protect the public from market externalities. While the medium may be new, the implications are not. Governments have grappled with analogous societal risks from terrorism for some time. Policy responses such as the Terrorist Risk Insurance Act (TRIA) can offer an instructive guide for governments to ensure catastrophic risks are being properly mitigated while minimizing moral hazards and the need for more direct government intervention in markets.

I will raise the prospect of government supported backstops like TRIA for state-sponsored cyber activities and offer considerations for discussion such as whether these are more likely to be effective as national or international efforts, the potential value and dangers of linking risk-reduction requirements to backstops, and the difficulty of determining when such backstops should be triggered (i.e., who determines what constitutes an act of war in cyberspace).