Transatlantic Cybersecurity: The Need for Regulatory Coordination

EU-US High Level Regulatory Cooperation Forum
April 11, 2013

Bruce Levinson
Levinson@TheCRE.com
The Center for Regulatory Effectiveness

"Cybersecurity regulation will take its place alongside environmental regulation, health and safety regulation and financial regulation

as a major federal activity."

-- CircleID 10/27/11

Cybersecurity Regulation includes Quasi-Regulatory Programs and Guidance Documents

Examples of US Cybersecurity Regulatory Programs which Need to be Coordinated with European Partners include:

- The Cybersecurity Framework for critical infrastructure companies being developed pursuant to Executive Order 13636
- The US Security and Exchange Commission's Cybersecurity Disclosure Guidance

Critical Infrastructure Companies Operate Internationally --
Uncoordinated National Regulation of Cybersecurity
Wastes Resources and Harms Security

The Cybersecurity Framework Should be Included in Regulatory Harmonization Discussions

- EU-US High Level Regulatory Cooperation Forum
- Transatlantic Trade and Investment Partnership (TTIP)

Center for Regulatory Effectiveness

- Established by former senior career officials from the White House Office of Management and Budget (OMB).
- Intervenes in Executive Branch proceedings to enforce the "Good Government" laws that "Regulate the Regulators."
- Acts only in its own name, not that of its sponsors.

Center for Regulatory Effectiveness: Cyber Policy Interventions

Examples include:

- The National Telecommunications and Information Administration's (NTIA's) supervision of ICANN (2004)
- Creating a National Cybersecurity Framework (2005)
- Creating a Cybersecurity Framework (2013)

Industry Leadership Should Drive Transatlantic Cybersecurity Coordination

- President Obama's Cybersecurity Executive Order 13636 emphasizes use of Industry Best Practices
- The international standards system is fundamentally a voluntary, industry-driven process
- Administration officials have emphasized the need for the Cybersecurity Framework to "Scale Globally"

Pro-Active European Participation in American* Cybersecurity Requirements is Essential

*When implemented, the Framework will impact globally-minded companies around the world.

Cost-Effectiveness:
The Prerequisite for Cybersecurity Regulation

Cost effectiveness needs to be designed into all critical infrastructure cyber defenses for two reasons:

1. Regulations must be cost-effective or they will not be viable and will not boost industrial security irrespective of legal requirements.

2. Cost effectiveness discussions must encompasses a review of several issues that are fundamental to any rational regulatory scheme starting which, what is meant by effective cybersecurity?

-- CircleID (9/10/12)

What is an Industry Best Practice?

NIST is directed to ensure maximum possible use of industry best practices in the Framework without possessing either:

- A definition of Industry Best Practices; or
- A federal compilation of industry best practices.

The Cybersecurity Framework Needs to Include a Process for the Federal Determination of Industry Best Practices

European-Based Industry Needs to Participate in Developing the Best Practice Determination Process

Determining Industry Best Practices: Guiding Principles

Global Diversity. The process should recognize the diversity of consensus and non-consensus cybersecurity Best Practices.

Affordability. The process to obtain federal acceptance of use of a Best Practice should be minimally burdensome.

Reciprocity. Cyber-defense measures undertaken at the behest of any EU or US agency should be accepted as an Industry Best Practice for purposes of the Framework.

Clarity. The best practices acceptance process needs to clearly define the operational boundaries to which the practice applies.

Recognition. The process should culminate, within a specified timeframe, in recognition of a company's Framework compliance.

Conformity Assessment: Self-Certification

The Conformity Assessment Process:

- Needs to take into account that companies may use varying combinations of a diverse Best Practices.
- Companies need to be able to obtain recognition for their entire package of compliance procedures.
- If companies have to hire expensive 3rd party auditing/ assessment organizations, the program won't work.

Self-Certification Backed by Appropriate Recordkeeping is the Only Economically Feasible Conformity Assessment Process