TSP Self-Regulation

Ben Wilson, JD CISSP
DigiCert & CA/Browser Forum

Chronology of Frameworks

1995 - 1996 –BS 7799 - EU Recommendation - Information Technology Security Evaluation Criteria (ITSEC), ABA Digital Signature Guidelines

1997-1999 – ETSI Guide - Trusted Third Parties, CP/CPS framework (ISO/TC68/SC 2 / RFC 2527), Gatekeeper CS2/CSPP for COTS Protection Profile

2000 -2003 – ANSI X9.79, WebTrust, ETSI TS 101 456, ISO 17799, ABA PKI Assessment Guidelines, ETSI TS 102 042

2005 - 2007 –CA / Browser Forum guidelines for EV SSL certificates, ISO 27001 and ISO 17799 -> ISO 27002

2011-2013 –ETSI TS 119 403 (EN 319 411-3), CABF Baseline Requirements, Security Requirements, WebTrust / ETSI, NIST Reference CP, and ENISA, ISO 27007/27008, etc.

Self-Regulation

Self-regulation as policy process: The multiple and criss-crossing stages of private rule-making, Tony Porter, McMaster University, Hamilton, Canada and Karsten Ronit, University of Copenhagen, Policy Sciences (2006) 39: 41–72

1. **Agenda-setting**
2. **Problem-identification (Rules Drafting)**
3. **Decision Making**
4. **Implementation**
5. **Evaluation**

Regulatory Agenda-Setting

1. **Agenda-setting**
   - What problems do we want to solve?
   - What kinds of changes are needed?
2. **Problem identification (Rules making)**

Identify problems in such a way that they can be addressed by modifications of practices, based on discussion or research of the existing standards of conduct that are deemed to be relevant.

Rules Drafting (Problem Identification)

Dependent heavily on:

- Influence of government in agenda setting stage
- Crafting a solution that is an incremental change to existing practice
- Choosing the “best practice”
- Great volumes of technical research (which sometimes can be arbitrary or political)
- Feasibility – capabilities of government and private sector

Decision Making

Is the proposed course of action appropriate? Will industry follow the recommended practice? Will industry be difficult to monitor?

- **TSP conduct** - complex knowledge, dispersed behavior (Internet crosses international boundaries)
- **Continuum of public-private influence** - there is an inflection point where government regulation reaches balance with private sector through communication and negotiation.

Government must address whether self-regulation allows negative externalities to persist unchecked.

Implementation

- Self-auditing and reporting play an important role. These mechanisms work where they have a degree of formality and sophistication.
- Encourage voluntary compliance - Appeal to industry's self-Interest in following best practices. Incentives and sanctions
- "Education" is an important part of implementation.
- "Education" can range from the publication of rules and "recommended practices on an association's website, to rigorous certification processes involving extensive studying and testing.

Evaluation

- Private rule-making is radical departure because regulation is public in character
- Private & public resources are often inadequate
- Annual reports on audit/improvements are good
- Problems must not become too severe before action taken -- failures need to be corrected.
- Transparency important, but a smooth resolution of internal conflicts between public regulation and private self-regulation.

Path Ahead

- Address security vulnerabilities by gathering information and following up
- Rules, Decisions, Implementation, Evaluation
- Improve coordination with government representatives, WebTrust, ETSI, and other key stakeholders
- Receive moral support for industry efforts
- Follow up with mild reporting expectations