Designing Effective Cybersecurity Regulations: Concepts, Misconceptions, and Innovations

Daniel Phelan
Research Associate
National Regulatory Research Institute
July 2015
Overview

- Cybersecurity is a complex, continually developing area seeing increasing regulation
- Fundamental misunderstandings can and have lead to unenforceable, misguided regulations
- Explain important concepts and clarify some misunderstandings that may inhibit the creations of effective regulations
- Examples of effective regulations from other sectors
Concepts

• Defense In Depth
  ○ Systems-based approach to security

• Advanced Persistent Threats (APTs)
  ○ Highly sophisticated attackers, limited defense abilities

• Bugs
  ○ Unknowingly present in almost all software
Concepts

- **Backdoors**
  - Intended to provide access to law-enforcement, but present tradeoffs

- **Zero-days**
  - Unknown exploitations, by definition impossible to defend against

- **Redundancy**
  - Two is one, one is none
Misconceptions

- Obscurity is security
  - Removing systems from the internet will not make them secure

- Cure-all solutions
  - Software vendors want to tell you that their systems are perfect

- Cyber 9/11
  - Change has already come, and will continue even without a drastic event
Misconceptions

- Technology is the answer
  - Employees are possibly the least secure piece of the puzzle

- Application of other regulations
  - NIST standards offer a guide to the thought process, but not the actual implementation

- Jurisdiction
  - Web servers controlled or located outside of your jurisdiction are difficult to regulate
Innovations

• EU Data Privacy
  ○ Directive 2002/58/EC asks EU member nations to conform to privacy standards for websites, personal data

• Payment Card Industry Data Security Standard
  ○ PCI DSS is enforced by the payment companies

• California Data Privacy
  ○ Creates rules for when a California resident accesses a website
Conclusions

- More innovations to be found, regulatory problem is not solved

- Critical infrastructure is a leader in this area, and other industries will look to our solutions

- Awareness of regulatory limitations and dangers will lead to enforceable, effective regulations