

# Top-Down Regulation

The key to progress on cybersecurity

Perry Pederson

# Outline

---

- ▶ Big picture on regulations
- ▶ Who thinks regulations are good?
- ▶ What is the industry's record?
- ▶ Summary
- ▶ Q&A



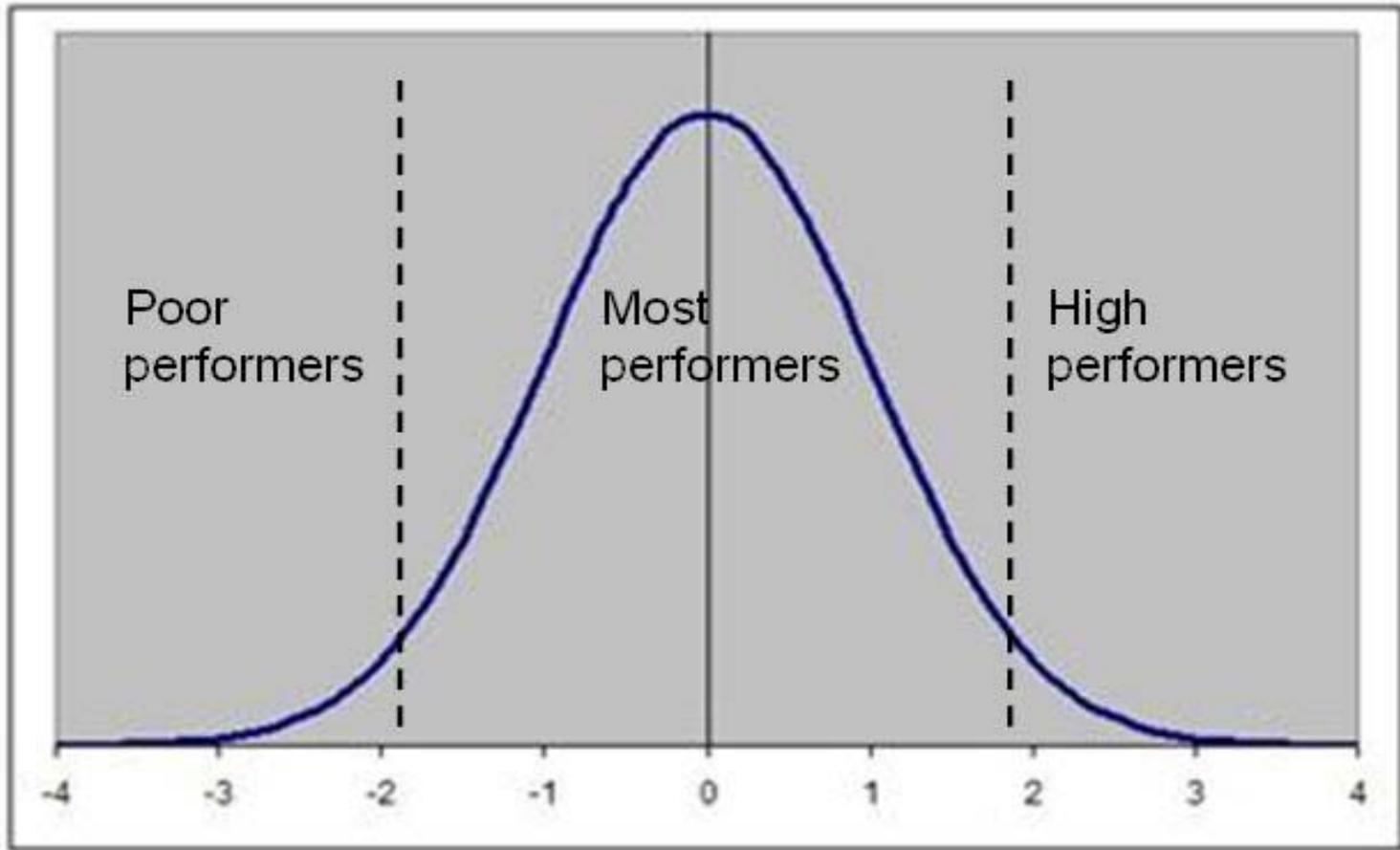
# Big Picture

---



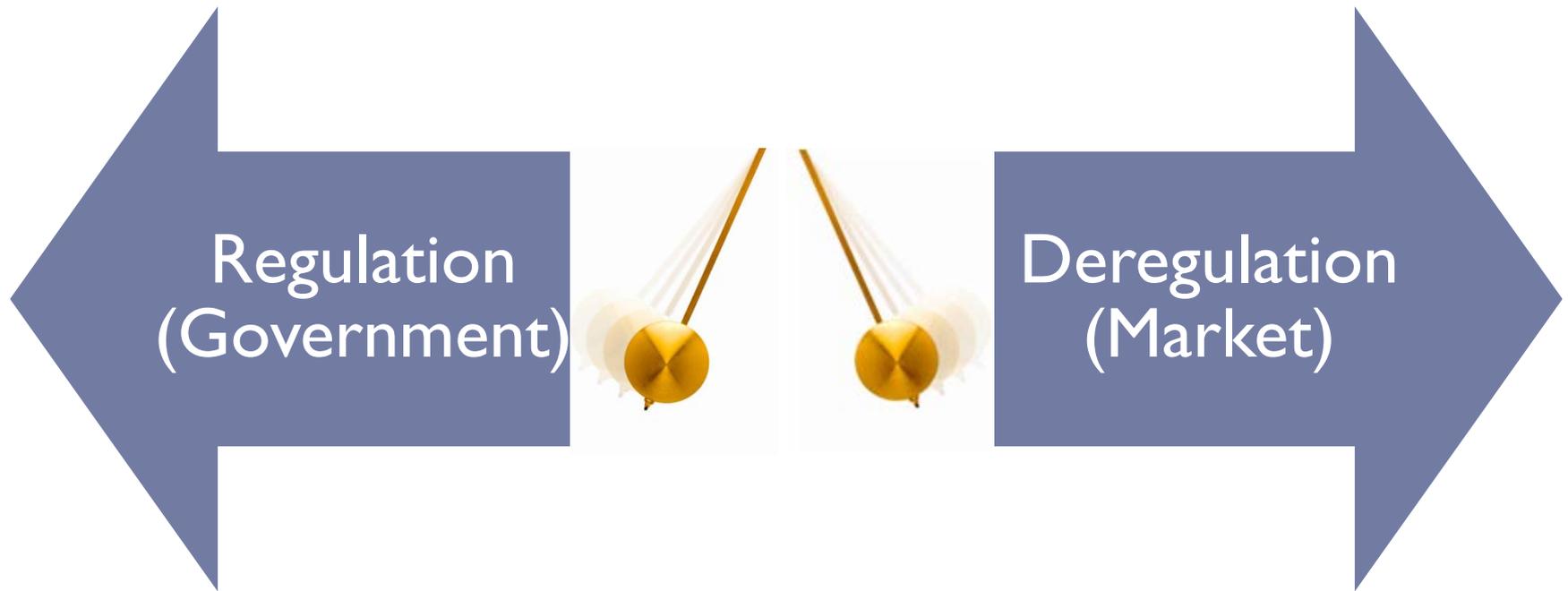
# Who are regulations for?

---



# The regulatory pendulum

---



# Regulations are good

---



# Ponemon Institute

## 2011 PCI DSS Compliance Trends Study

---

- ▶ A key finding from this research is that there is a **dramatic difference** in the number of data breaches experienced by organizations considered compliant with PCI DSS [Payment Card Industry Data Security Standard] and those that are not compliant.



# National Infrastructure Advisory Council (NIAC)

---

- ▶ NRC holds nuclear power plants to the highest security standards of any American industry.
- ▶ High regulation among a small number of owners and operators gives the nuclear sector strong resilience.
- ▶ The nuclear sector is one of the most regulated of the CIKR, its risk analysis and risk management practices are highly developed, and its facilities are **very robust and hardened**.



# ISSA Journal – Donn Parker

---

- ▶ Compliance: We are finding that the growing body of security **compliance** legislation such as SOX, GLBA, and HIPAA and the associated personal and corporate liability of managers is rapidly becoming a **strong and dominant security motivation.**



# Joe Scalone

---

- ▶ Regulatory Compliance (RC) is a treasure trove of value. From better business intelligence to improved security, the benefits of RC abound. The key is to understand the payback and how to get it.
- ▶ It is a mistake to view costs of RC as greatly outweighing the benefits.
- ▶ Aside from the overarching societal benefits from corporate accountability there are **abundant economic and business benefits** for those companies who choose to harvest such fruit.



# What is the industry record?

---



# National Academy Conference

---

- ▶ “Here is a case in which the government can’t carry out its most basic mission – providing security – without the cooperation of the private sector. And here is a case in which the private sector will quickly need a range of products on which the market has never before put a premium – the classic **market failure** that calls out for government involvement.” - Congressman Boehlert



# Richard Clarke

---

- ▶ “Last year was a **market failure** in cybersecurity and 2004 doesn’t look much better. In general Internet Service Providers (ISPs) do nothing about security. The market isn’t forcing the ISPs to do anything about security.”



# NERC

---

- ▶ NERC testified to Congress that 75 percent of the identified vulnerabilities had been addressed -- and then **failed** to deliver data to support that assertion.
- ▶ "What do you think we are, a bunch of jerks?" asked Rep. Bill Pascrell.
- ▶ Pascrell called for NERC to be held in contempt of the committee for delivering misleading testimony about the state of the utilities' cyber defenses.



# DOE OIG audit of FERC

---

- ▶ Recent testimony before Congress disclosed various issues, including the existence of significant vulnerabilities in the power grid's infrastructure and many utilities that were **not in compliance with the standards**.
- ▶ We found that these problems [lack of critical asset determination, lack of controls, lack of prioritization] existed, in part, because the Commission had only **limited authority** to ensure adequate cyber security over the bulk electric system.



# Joe Weiss

---

- ▶ “The electric industry has demonstrated they cannot secure the electric infrastructure without regulation. Other industrial verticals have similarly defaulted. Therefore, **regulation is needed.**”



# Pending Cyber Security Bills

---

- ▶ **HR 76**

- ▶ Cybersecurity Education Enhancement Act of 2011

- ▶ **HR 174**

- ▶ Homeland Security Cyber and Physical Infrastructure Protection Act of 2011

- ▶ **HR 1136**

- ▶ Executive Cyberspace Coordination Act of 2011

- ▶ **S 21**

- ▶ Cyber Security and American Cyber Competitiveness Act of 2011

- ▶ **S 372**

- ▶ Cybersecurity and Internet Safety Standards Act

- ▶ **S 413**

- ▶ Cybersecurity and Internet Freedom Act of 2011
- 



# Summary

---

- ▶ Regulations are necessary
- ▶ Regulations are good



# Q&A

---



Preparing for the next regulatory appraisal.

---

