

RSA[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: PNG-W09

Nanny State to Invisible Hand: What's the Proper Role for Regulation?



MODERATOR: **Gib Sorebo**

Security Consulting Senior Manager
Accenture
@gibsorebo

PANELISTS: **Lauren Topelsohn**

Member
Mandelbaum Salsburg P.C.

Kathryn Coburn

Partner
Murphy Cooke Kobrick LLP

John Gregory

General Counsel (retired)
Government of Ontario, Canada
@johndgregory

#RSAC

Session Agenda

- Introduction of topic and panelists and highlight objectives of the session
- Review the typical goals of regulation and common law negligence principles
- Survey examples of cybersecurity laws, regulations globally, and common law principles
- Examples of case law and regulatory action
- Evidence (or lack thereof) to support improvements in cybersecurity
- Assessment of what incentives/penalties/assistance work and what other options should be considered
- Call to Action

Are these laws and regulations effective?

How do we better incentivize more secure behaviors?

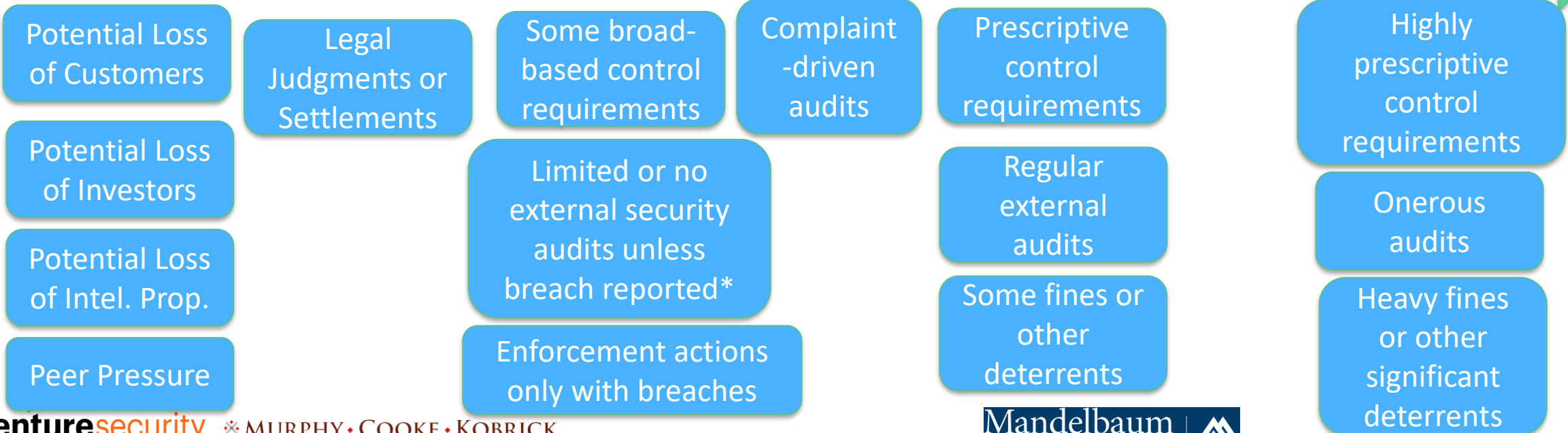
The Legal/Regulatory Landscape for Cybersecurity

Regulation/Non-Regulatory Drivers

| | | | | | | |
|-----------------------------|----------------------------|------------------|----------------------|-------------------------------------|------------------|--------------------|
| Market-based risks | Sarbanes-Oxley | Insurance-driven | Export Control/CFIUS | FISMA/800-171 (govt contractors) | FISMA (civilian) | FISMA (DOD) |
| SEC Disclosure Requirements | Common Law Torts/Contracts | FTC Actions | MA/MN Breach Laws | German IT Security Act | PCI DSS | NERC CIP |
| | FERPA | EU NIS Directive | | HIPAA | | |
| | FCRA | CCPA | | GLBA & related financial serv. regs | | Nuclear Power Regs |
| | Most State Breach Laws | GDPR | | | | |
| | | PIPEDA | | | | |
| | | CFATS | | | | |
| | | BASEL II/III | | | | |



Incentives/Motivators



*Excludes broad-based financial audits of public companies by hired external auditors