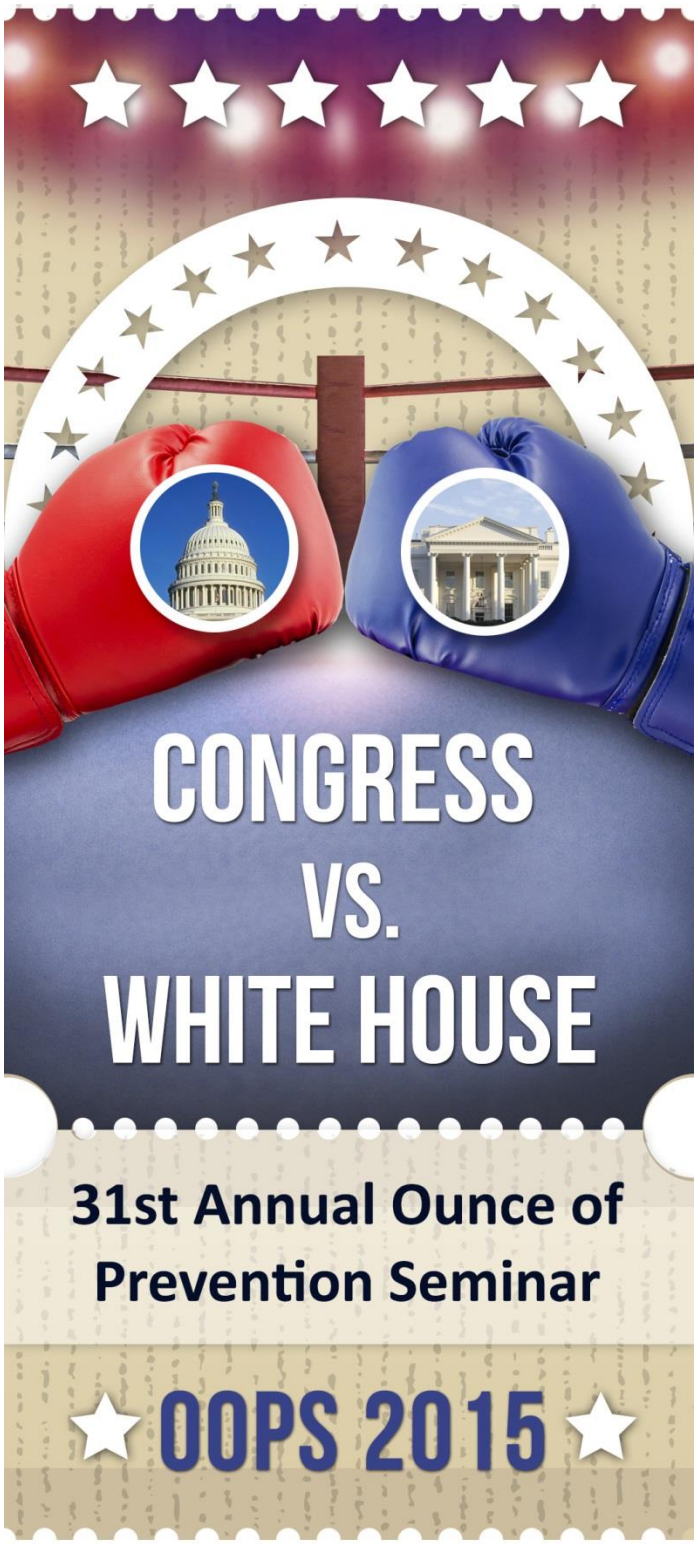


crowell moring

CYBERSECURITY RISK MANAGEMENT

Evan Wolff
Maida Lerner
Peter Miller
Kate Growley

Roadmap

- Cybersecurity Risk Overview
- Cybersecurity Trends
- Selected Cybersecurity Topics
  - Critical Infrastructure
  - DFARS Safeguarding Rule
  - Internet of Things
- Assessing and Managing Cybersecurity Risk

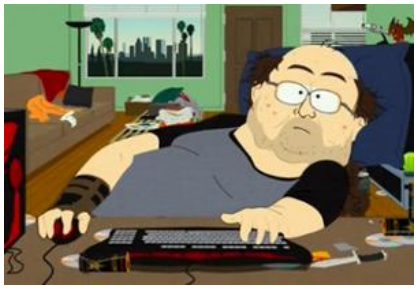
Cybersecurity Risk Overview

crowell moring

What Are The Threats?

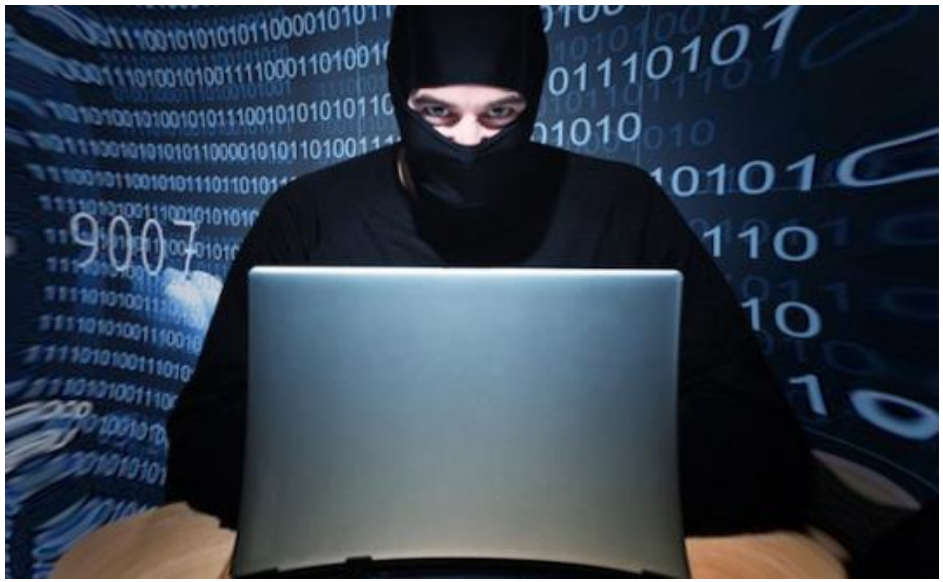
- Insider threats
  - ✓ Snowden
  - ✓ Negligent employees
- Vendors/Supply Chain
  - ✓ Target
- Nation States
  - ✓ China
  - ✓ Russia
  - ✓ Iran
- Hacktivists
- Organized Crime
- Dude in his Mom's basement

TARGET



What Are They After?

- Intellectual property/trade secrets
- Damage and disruption to infrastructure
- Financial gain (PCI, PII, PHI)
- Reputational harm (email)
- National security impact



What are the Potential Consequences?

- Claims and Recovery
  - Negligence
  - Breach of Contract
  - Unfair Trade Practices
  - Tort Claims
  - Federal privacy and cybersecurity laws
  - State laws – e.g., CMIA
  - Shareholder actions
- Direct impact/business harm
- Reputational harm
- C-Suite impact

Cybersecurity Trends

Cybersecurity Trends

- Increased White House Involvement
  - Summit on Cybersecurity and Consumer Protection
  - Executive Orders, Legislation
- More Federal Entities, More "Guidance," More Compliance Challenges
  - Alphabet Soup: DOD, DOJ, DHS, HHS, FAA, FCC, FDA, FTC, CFPB, SEC, NIST, NTIA, OIGs...
- Reporting Cybersecurity Incidents: "Gotcha" or Centralized Clearing House?
  - Criminal authorities
  - Federal regulatory authorities
  - State authorities

Cybersecurity Trends (cont.)

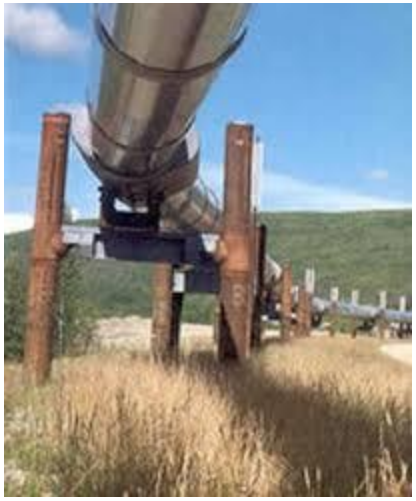
- More Legislative Initiatives
  - Federal and state legislative focus – hearings and bills
  - Tension between federal and state authority
- More Litigation
  - Federal and State Enforcement Actions
  - Breach Litigation (Sony/Anthem)
  - Victim or Defendant?
- Public/Private Collaboration
- Insider Threat Initiatives

crowell moring

Cybersecurity and Critical Infrastructure

Critical Infrastructure Vulnerabilities

- Infrastructure is aging and becoming obsolete.
- Industrial Control Systems and Supervisory Control and Data Acquisition Systems were built with efficiency and safety – NOT SECURITY – in mind.
- Use of commercially available ("off the shelf") ICS and SCADA technology reduces costs but increases vulnerability.
- On/Off operation and lack of redundancy



Scary Times for Critical Infrastructure…

- 100 % increase in attacks on SCADA systems in 2014.
  - 2015 Dell Security Annual Threat Report
- In 2014, ICS-CERT received and responded to 245 incidents reported by facility and asset owners.
  - ICS-CERT Monitor (9/2014-2/2015)
- Several foreign governments have already hacked into U.S. energy, water and fuel distribution systems.
  - NSA Director Rogers testimony before House Intelligence Committee (11/2014)

Federal Initiatives to Improve Critical Infrastructure

- Obama Administration recommended $15 billion in new spending programs or tax credits to carry out a major overhaul of the nation's energy infrastructure (April 2015 Quadrennial Energy Review).
- Executive Order 13631 (Improving Critical Infrastructure Cybersecurity) – shifted federal government's regulatory focus to voluntary, risk-based standards.

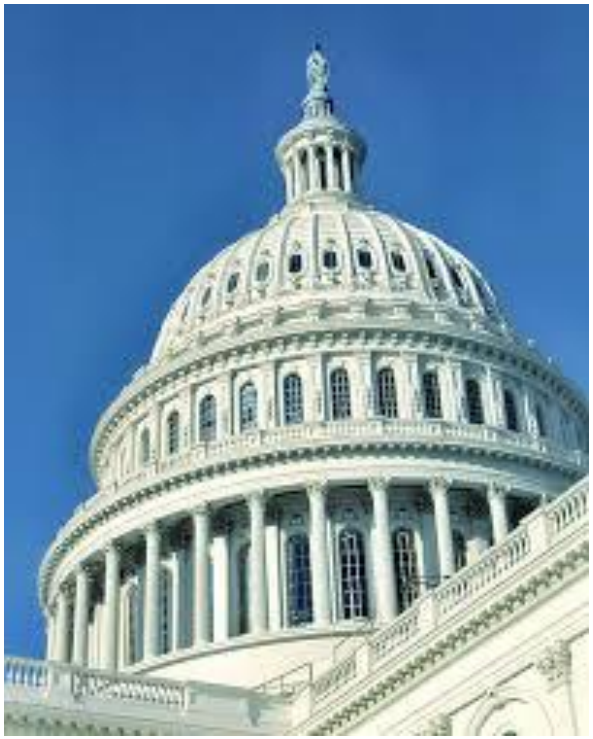
Federal Initiatives to Improve Critical Infrastructure (cont.)

- NIST Cybersecurity Framework
  - Core: Activities to help organizations address cybersecurity risks and respond to and recover from cyber-attacks
  - Tiers: Metric to help organizations assess their implementation of Core
  - Profiles: Snapshot of risk management posture (e.g., "as-is" and "to be")

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Critical Infrastructure Regulations and Best Practices

- Chemical Facility Anti-Terrorism Standards (CFATS)
- The Maritime Transportation Security Act (MTSA) regulations
- FERC's Critical Infrastructure Protection (CIP) Standards
- Transportation Security Administrative (TSA) Pipeline Security Standards



Risk Reduction for Critical Infrastructure

- Risk-based cybersecurity program, including governance framework
- Risk management tools (SVAs and SSPs)
- Vendor management agreements
- Cybersecurity training and reporting
- Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 ("SAFETY Act")
- Cybersecurity insurance
- Cybersecurity Framework
- Public and private information-sharing opportunities
- Familiarity with cybersecurity trends, standards, and best practices

crowell moring

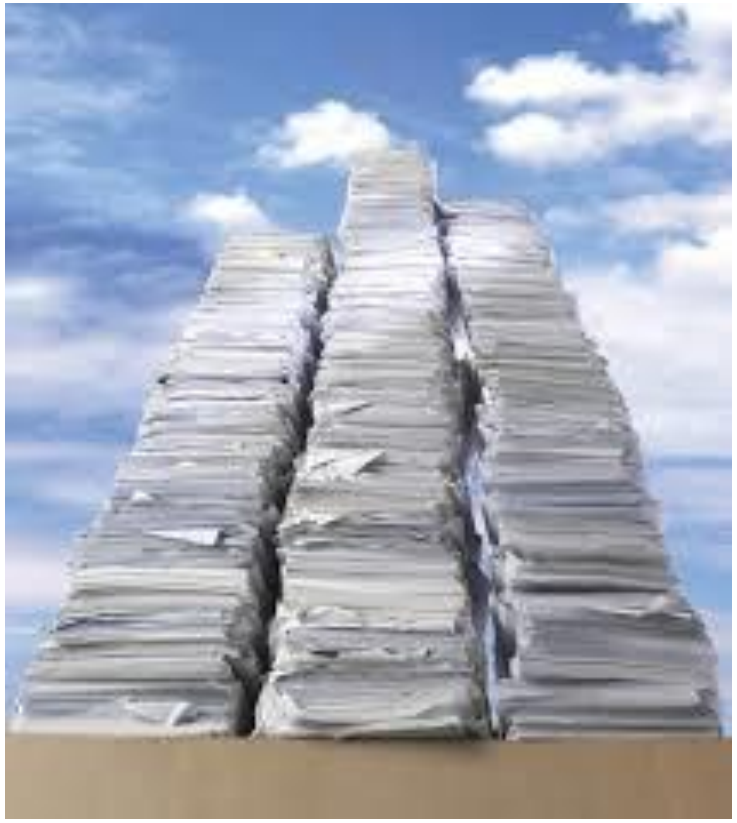
Cybersecurity and DFARS

What's the DFARS Safeguarding Rule?

- Incorporated into all defense contracts with mandatory flowdowns
- Applicable to defense contractors with controlled technical or scientific information on their information systems
- Requires "adequate security" and cyber incident reporting

What's New Since Last Year?

- Procedures, Guidance, and Instructions 204.73 (12/2014)
- Guidance to Requiring Activities for Implementing DFARS Clause (2/2015)
- DoD Memorandum on DFARS Compliance (2/2015)



What Should I Know Up Front?

- Uncertain whether actual presence of technical information triggers requirements
- DoD responsible for noting when contract involves technical information

Is There Anything New About Reporting?

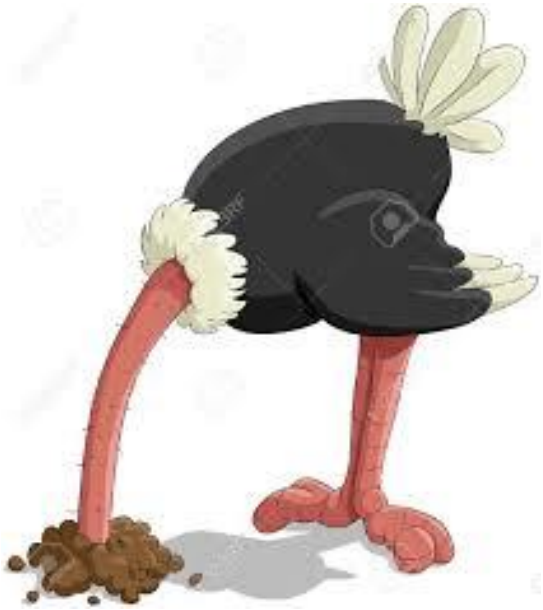
- Report as much as possible and supplement later
- Subs report to primes, and primes report to DoD
- Additional DIB reporting voluntary

What Happens After I Report an Incident?

- DoD may request self-assessment of DFARS compliance and vulnerabilities
- Suffering cyber incident does not mean you're non-compliant
- Failure to implement adequate security constitutes breach of contract

What If My Contracts Don't Have the DFARS Safeguarding Clause?

- Not retroactive
- Expect a contract modification



crowell moring

Scorecard for DFARS Clause 252.204-7015

Component	2015-Q1	2015-Q2	2015-Q3
Army	33%		
Department of Navy	46 %		
Air Force	22%		
DLA	82%		
DCMA	2%		
ODAs			
Total	65%		

Scorecard Goal		
Status	Lower	Upper
Green	92	100
Yellow	85	< 92
Red	0	< 85

256

Cybersecurity and the Internet of Things

Defining (?) the Internet of Things

- IoT "refer[s] to 'things' such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet.

  FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015)

- IoT is a "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."

  Cloud Security Alliance, *Security Guidance for Early Adopters of the Internet of Things (IoT)* (April 2015) (quoting International Telecommunications Union Recommendation ITU-T Y.2060 (June 2012))

- "It really ought to be called the Internet of Things and Humans."

  Tim O'Reilly, radar.oreilly.com (April 16, 2014)

Internet of Things – Cybersecurity Challenges

- Absence of regulations, standards, and best practices
- Ease of market entry
- By design, IoT devices interact with other devices, networks, and systems with limited oversight and limited user involvement
  - Limited ability to control data flow
  - Limited ability to detect unauthorized users and unauthorized data access
- Difficulty of detecting and remediating security flaws in deployed devices
- Security vulnerabilities result not only from individual devices and systems, but also from interactions among devices, systems, and users
- Responsibility for detecting, reporting, and remediating IoT incidents
- IoT vulnerabilities already being exploited

Cybersecurity Risk Management

Assessing and Managing Cybersecurity Risk

1. Identify and Classify Sensitive Data and Regulated Systems
2. Establish Clear Governance
3. Review and Update P&P
4. Prepare for an Incident
5. Review Vendor Management Process
6. Analyze Audit and Reporting Processes
7. Conduct Training
8. Participate in Industry and Government Partnerships
9. Implement Controls to Protect Data and Systems

Questions?

Peter Miller
202-624-2506
pmiller@crowell.com

Evan Wolff
202-624-2615
ewolff@crowell.com

Maida Lerner
202-624-2596
mlerner@crowell.com

Kate Growley
202-624-2698
kgrowley@crowell.com