BakerHostetler

THE CHERTOFF GROUP

LOCKTON®

Implementation of the Cybersecurity Executive Order

November 13th, 2013

Ben Beeson, Partner, Lockton Companies
Gerald J. Ferguson, Partner, BakerHostetler
Mark Weatherford, Principal, The Chertoff Group

Mark Weatherford is a Principal at The Chertoff Group and advises clients on a broad array of cybersecurity issues. As one of the nation's leading experts on cybersecurity, Mr. Weatherford works with organizations around the Nation and the world by creating comprehensive security strategies for core business operations and objectives.

Prior to joining The Chertoff Group, Mr. Weatherford was appointed by President Obama as the Department of Homeland Security's first Deputy Under Secretary for Cybersecurity.

Gerald J. Ferguson

BakerHostetler

Jerry Ferguson serves as the Coordinator for the Intellectual Property, Technology and Media Group in BakerHostetler's New York office and as the National Co-Leader of BakerHostetler's Privacy and Data Protection Team.

Since the enactment of the first modern privacy and data protection statutes in the 1990s, Jerry has assisted hundreds of clients in creating and implementing national and global privacy and data protection policies. He has extensive experience advising companies suffering data security breaches that may trigger obligations under state and federal breach notification laws.

Ben Beeson
Lockton Companies

Ben leads the Global Technology and Privacy Practice at Lockton based in London.

A team of associates in the USA, Europe and Asia assist Lockton clients in dealing with emerging intangible risks including cyber, technology intellectual property and supply chain.

Ben is directly involved in advising both the US and UK governments as to how the insurance industry can support improved cyber security for critical infrastructure industries.

Evolution of Concern

- One of my gauges of the importance and security maturity of a company is by identifying who is most concerned .
  - If it's the CISO or the CIO, there's a problem.
  - If it's the CEO or the Board - there's hope.
- We're finally starting to see an evolution of concern and awareness about security

Legislation

Over 50 different pieces of Legislation introduced in the past two years. In the 113th Congress:

- H.R. 624 - Cyber Intelligence Sharing and Protection Act (CISPA) – Rogers
- S.??? - Senate version of CISPA – Chambliss and Feinstein
- H.R. 1163 – Federal Information Security Amendments Act of 2013 (FISAA) – Issa
- Discussion Draft - National Cybersecurity and Critical Infrastructure Protection Act (NCCIP Act) of 2013 – McCaul
- S.1353 - Cybersecurity Act of 2013 - Rockefeller
- S. 21 - Cybersecurity and Cyber Competitiveness Act of 2013 - Rockefeller
- H.R.756 – Cybersecurity Enhancement Act of 2013 - McCaul

Executive Order 13636

Cybersecurity Standards	• Requires development of a Cybersecurity Framework • Develops voluntary critical infrastructure cybersecurity program and proposes incentives • Identifies regulatory gaps
Privacy	• Mandates strong privacy and civil liberties protections • Directs regular assessments of agency activities
Information Sharing	• Expands the voluntary DHS Enhanced Cybersecurity Service (ECS) program. • Expedites private sector threat reporting, both classified and unclassified. • Expedites issuance of security clearances to critical infrastructure members in the private sector

The Sins and the Sinners

Sins

The Sins fall into 3 basic categories:

1. Cyber-espionage
2. Cyber-crime
3. Cyber-hacktivism

Sinners

And the Sinners are:

1. Nation States
2. Criminal Groups
3. Hacktivists and Terrorists

Et tu Brute?

- One of the most recurring conversations I have is, "I didn't think we were:
  - big enough
  - important enough
  - valuable enough

  to be concerned about hackers."
- It's like Caesar when he heard the *'Ides of March'* premonitions. He recognized the omens … he just didn't think they applied to him.

Context of the Order

BakerHostetler

Congress Has Failed to Enact National Cybersecurity Law

- Federal Security Standards Concerns
- Information Sharing Concerns
  - Republicans: Liability Limitation
  - Democrats: Civil Liberty Concerns

Characteristics of the Order

Vague

- Material Terms not defined or discussed
- Intentionally vague?

Specific Action Deferred

- Review, Comment, Report

What is Critical Infrastructure?

Defined Broadly and Generally (Section 2)

- Secretary of Homeland Security Will Identify Key Threats (Section 9)
  - Communications, Manufacturing, Energy, Food and Agriculture, Financial, Healthcare Transportation, Shipping
  - Critical Infrastructure Partnership Advisory Council www.dhs.gov/council-members-critical-infrastructure-partnership-advisory-council

Developing the Cybersecurity Framework

BakerHostetler

- NIST was given 240 days (mid-October) to publish a "preliminary version" of the Cybersecurity Framework.
- The final Framework must be complete by mid-February, 2014

"The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess and manage cyber risk."

Framework Development

- Cybersecurity Framework defined as “set of voluntary standards and best practices to guide industry in cyber risks.”
- Order directs NIST to “engage in open public review and comment process” in developing the Framework involving all stakeholders in public and private sectors.
- Patrick Gallagher, NIST Director:

> *“Framework will not be a NIST work product; it will be developed by and belong to private industry.”*

Preliminary NIST Cybersecurity Framework

BakerHostetler

- Preliminary version released October 22, 2013: http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
- Core: five functions
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- For each, categories, e.g., Asset Management, and subcategories, e.g., inventorying of software platforms and applications
- Profile: establishing an organizational road map to get from here to there, i.e., substantially reduced cyber risks
- Implementation Tiers: (i) partial; (ii) risk-informed; (iii) risk-informed and repeatable; (iv) adaptive

Preliminary NIST Cybersecurity Framework

BakerHostetler

- Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program
  - Quite detailed outline of best practices for handling PII
  - Criticized for imposing government standards on industry

Issues for Further Development

i. Authentication;

ii. Automated indicator sharing;

iii. Conformity assessment;

iv. Data analytics;

v. International aspects, impacts, and alignment;

vi. Privacy; and

vii. Supply chains and interdependencies.

Voluntary or Industry Standard

- May be Implemented by Resolution Under Statutory Authority
  - Financial Institutions
  - Utilities
- Authoritative Source
- Extensive Industry Interactive
  - Over 3,000 industry comments
  - Four workshops
- Consistent with Security Literature

Responding to NIST Framework

- Revise Policies To Reflect Language of The Framework
- Make Policies “Adaptive”
  - Identify new threats
  - Revise
  - Evaluate
- Senior Management Must Drive Process

DoD Information Sharing

- From 2010 Defense Industrial Base ("DIB") Pilot
- Companies must apply to be approved
- Approved companies receive threat information they can use to protect their systems
- Participating companies must share threat information back with the Government to be shared with other participants
  - DoD will undertake reasonable efforts to anonymize before sharing
  - DoD will resist FOIA disclosure requests to the extent permitted by law

DIB Information Sharing

- Pluses
  - Greater threat information
  - Preferred consideration in government contracts
- Minuses
  - Loss of control of information
    - FOIA uncertainty
    - May not be sufficiently anonymized
  - DoD may use info to assert contract breach and for law enforcement purposes

Other Information Sharing

BakerHostetler

- Regulatory Initiatives
  - Treasury Cyber Intelligence Group
  - Financial Services Information Sharing and Analysis Center
  - Federal Energy Regulatory Commission
  - Enhanced Cybersecurity Services Program
- Liability Concerns From Information Sharing
- Blaming the victim: Emerging Liabilities
  - SEC enforcement
  - Shareholder suits
  - Third Party contract claims

Cyber Insurance Marketplace & Cyber Security Impact

White House Cyber Insurance Meeting Discussion Topics:

- Cyber Security Privacy
- Civil Liberties and Policy
- National Security
- Government Approach
  - Cyber Security Incentives
    - Cyber security Insurance
    - Grants
    - Process Preference
    - Liability Limitation
    - Streamline Regulations
    - Public Recognition
    - Rate Recovery for Price Regulated Industries
    - Cyber Security Research
- National Institute of Standards and Technology (NIST) Framework

At the White House on August 26, 2013

What are Cyber Risks?

Ubiquitous

Sabotage

Espionage

Operational

Data Security and Privacy

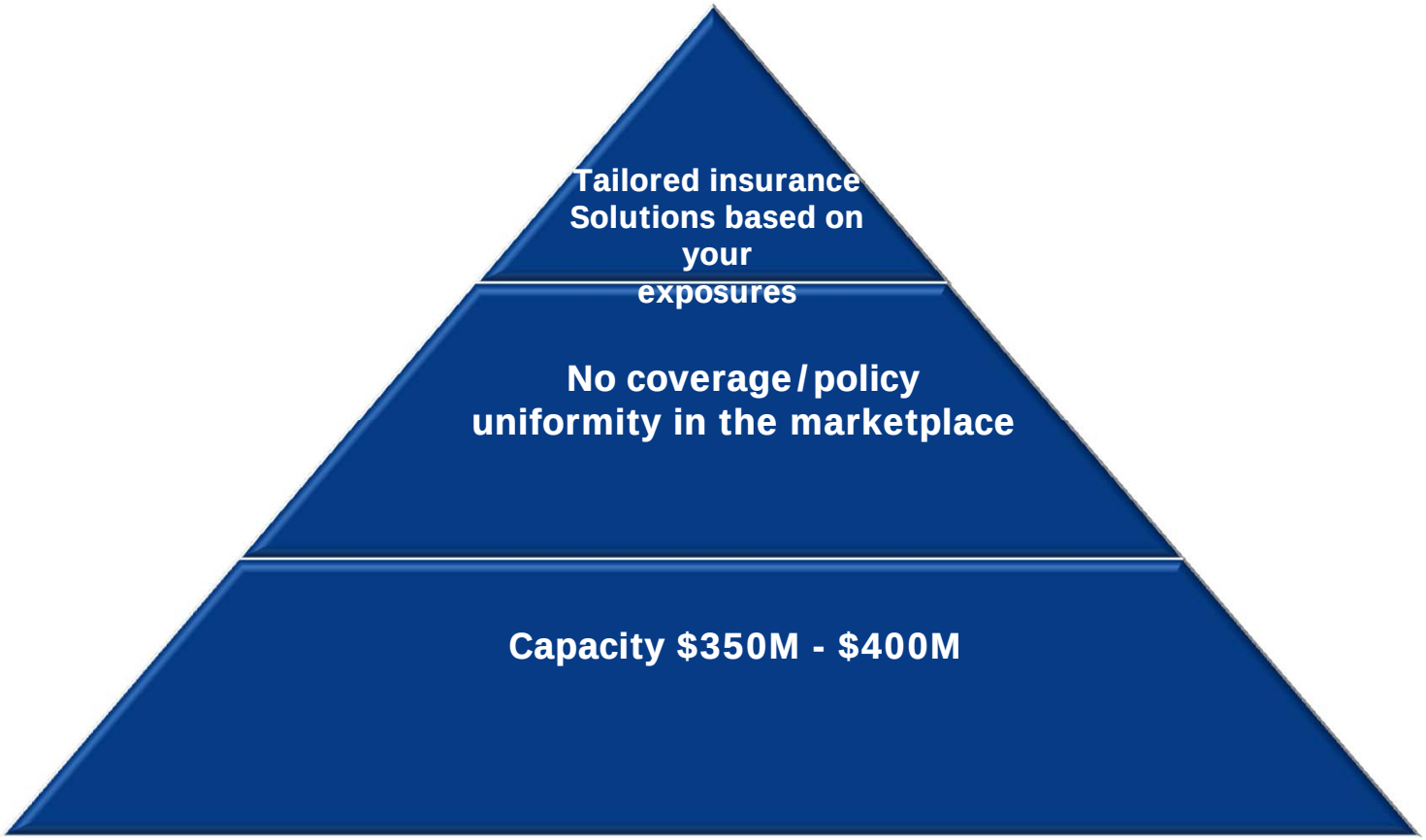
Media

Tech

Data Security and Privacy

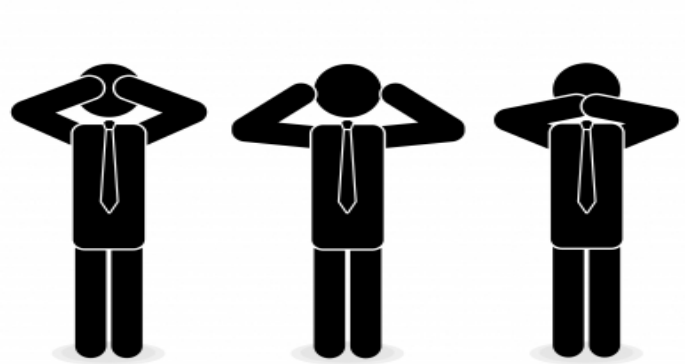
- Data Breach Response Costs
- Privacy Regulatory Action
- Civil Litigation
- **INSURABLE**

Cyber Insurance Marketplace



Operational Risk

- Network outage from non-physical trigger and non-tangible loss
  - Includes dependent business interruption to cloud providers or other vendors
- Loss of Revenue
- Extra Expense
- **INSURABLE**



Cyber Espionage

- Who? *State Sponsored or Organized Crime*
- What? First Party Loss of Intellectual Property
- **UNINSURABLE**

Operational Risk - Cyber Sabotage

- Non physical damage and physical damage business interruption.
- Property Damage
- Bodily Injury

- Stuxnet
- Flame

- **PARTIALLY INSURABLE**

One Broker's Response…

Cyber insurer policies vex energy firms, says Marsh

4 September 2013 | By Newsdesk

Print Email Share Comment

CL380 clauses often a problem

Uncertainty around cyber exclusion clauses is eroding the value of insurance and worrying global energy firms, according to Marsh.

RELATED ARTICLES

How the digital revolution has left firms exposed
19 July 2013

Marsh: 33% more US firms buying cyber cover
15 March 2013

Cyber-attack threats on the increase, warns Munich Re
28 November 2012

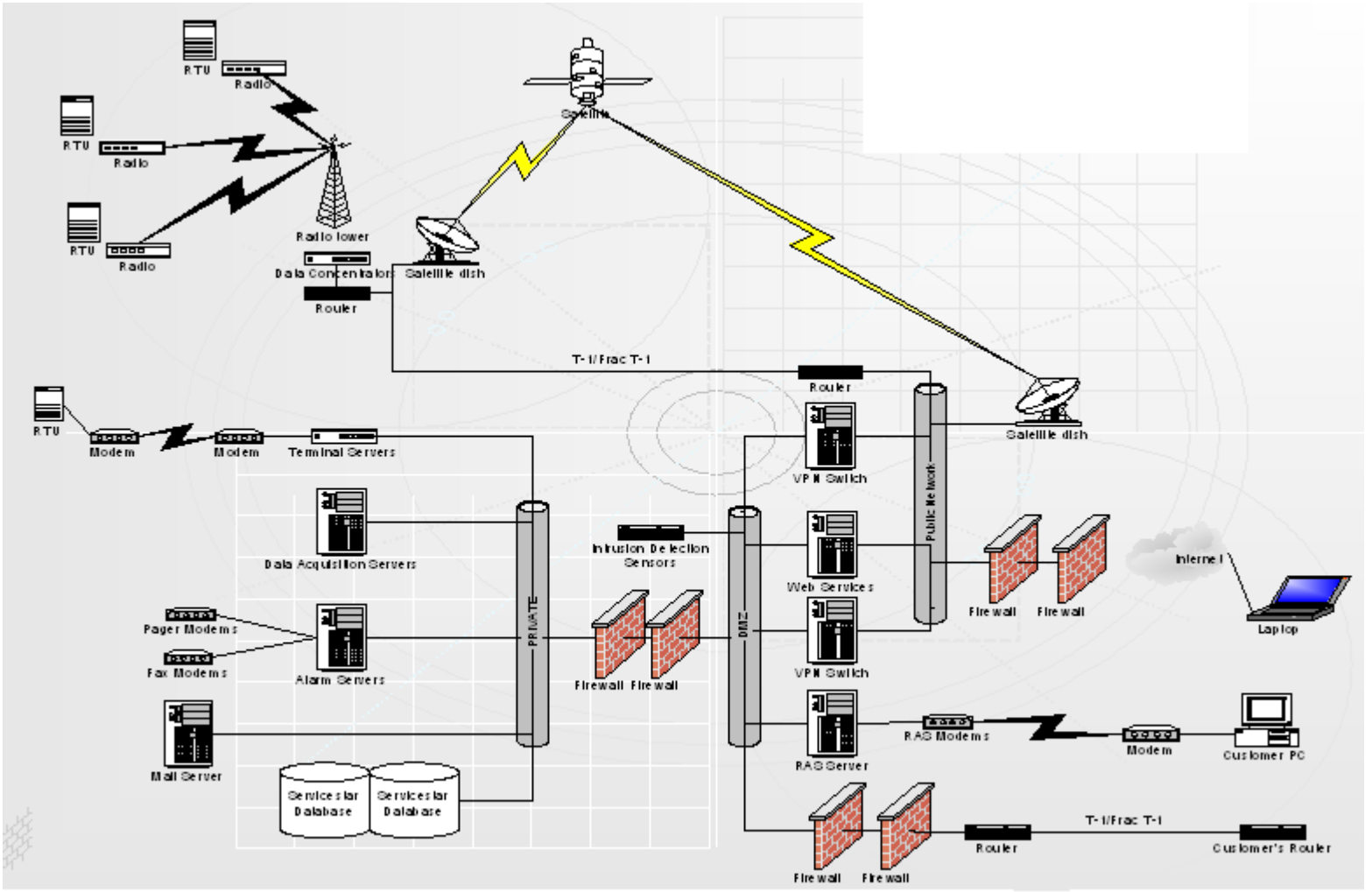
Risk Atlas: Cyber crime
18 October 2011

What is CL380?

CL380

10/11/03.
INSTITUTE CYBER ATTACK EXCLUSION CLAUSE
1.1. Subject only to Clause 1.2. below, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.
1.2. Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system an/or firing mechanism of any weapon or missile.

SCADA – Automating Processes



Insured Events

- Accidental Damage or Destruction
- Administrative or Operational Mistakes
- Computer Crime and Computer Attacks
  - Denial of Service/Distributed Denial of Service
  - Malicious Code
  - Unauthorised Access
  - Unauthorised Use

Indemnity

What does SCADA product cover

- Business Interruption caused by an insured peril
- Business Interruption as a result of property damage caused by an insured peril
- Property Damage (on a case by case).
- Digital Asset Damage

What does SCADA product NOT cover

- Bodily Injury
- Technology Service Errors & Omissions
- Seepage and Pollution or TPL