Cybersecurity: The Legal, Legislative and Regulatory Outlook

Jamie Barnett
Rear Admiral USN (Retired)
Co-Chair, Telecommunications
Partner in Cybersecurity Practice

VENABLE®
ATTORNEYS AT LAW

Cybersecurity Impact and Costs

- Direct Financial Costs
- Reputational Damage
- Loss of Intellectual Property, Business
- Government Fines/Regulatory Oversight
- Class Actions

Cybersecurity Legislation

- National Cybersecurity Protection Act of 2014– codifies the NCCIC at DHS
- Cybersecurity Enhancement Act of 2014 (Sen. Rockefeller)– NIST authorization for Framework and research
- Federal Information Security Modernization Act of 2014– reforms 12 yr old FISMA from a checklist to ongoing diagnostics
- DHS Cybersecurity Workforce Recruitment and Retention Act– fast-track the process of hiring cyber professionals at the agency and offer new hires a competitive salary
- Cybersecurity Workforce Assessment Act – DHS will assess cyber workforce every 3 years
- Cromnibus: Cyber spending goes up for DOJ, DOD, DOE (from $25M to $304M), but frozen for DHS

Liability from Cyber Attacks

- Depending on the type of attack, victims may be subject to:
  - Third-party liability:
    - Claims alleging negligence
    - Contract claims
    - Shareholder suits
    - Enforcement actions
  - First-person liability:
    - Business losses
    - Loss of share value
    - Remediation costs (identity protection, card replacements, PR expenses, etc.)

VENABLE® ATTORNEYS AT LAW

Is There a Cyber Standard of Care?

Bethesda AFCEA Chapter

- Some courts have indicated willingness to hold cyber victims liable to consumers for breaches where security practices were not reasonable
  - Obstacles do still exist, e.g. legal standing and "economic loss" rule
- FTC unfairness-based enforcement actions can serve as indicators of unreasonable practices
- The NIST Framework is being closely scrutinized to see if it becomes the "gold standard" for all companies
  - *See, e.g., Shames-Yeakel v. Citizens Financial Bank*, 677 F.Supp.2d 994, 994 (N.D. Ill. 2009).
  - At least one court dealing with a data breach lawsuit determined that failure to use "industry-standard encryption" was grounds for allegation of failure to provide reasonable data security measures
  - Recent PWC report found 29% of respondents had already implemented NIST CF and 25% said adoption was a future priority

VENABLE® ATTORNEYS AT LAW

Is There a Cyber Standard of Care?

Bethesda AFCEA Chapter

Cybersecurity Framework does not provide a safe harbor, but adoption could provide evidence of diligence and care to follow best practices

Kelly Welsh, General Counsel
Department of Commerce
(to Chamber of Commerce and ITIC)

Cybersecurity Framework may be a defense to liability suits

Toward a Cybersecurity Duty of Care? Exploring the Implications of the 2014 Cybersecurity Framework on Defining Best Practices and Shaping Negligence Law
draft article for Texas International Law Journal

Cyber Insurance is Going Mainstream

- New data breaches are being announced increasingly frequently
  - Retailers, banks, etc.
  - North American entities reported 11% more incidents this year over last
- U.S. cyber insurance market could hit $2 billion in gross written premiums this year – twice that from 2013
- Estimated average financial loss due to cybersecurity incidents from 2013-2014 was $2.7 million, an increase of 34%
  - For organizations with revenue over $1 billion, the average cost was $5.9 million, up $2 million from prior year

VENABLE®
ATTORNEYS AT LAW

Cybersecurity Regulation

Bethesda AFCEA Chapter

- Executive Order 13636 and government contracts
- SEC examines cyber preparedness of Wall Street
- Energy Sector: CIP Cyber requirements and DOE tying IT asset management to cybersecurity
- Communications: FCC Chairman's speech in June 2014
  - More than what the market will bear
  - Less than heavy handed regulations
  - But mentions 'accountability' about 6 times
  - Watch for the CSRIC report in March, 2015

Cybersecurity Framework

- Leverages existing cybersecurity best practices (ISO 27001/2, SP800-53, COBIT, ISA 99, etc.).
- Controls divided into five “core functions”:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Each function has categories, sub-categories, and informative references.
- Tiers represent how orgs view and respond to risk; profiles facilitate customization and improvement

VENABLE®
ATTORNEYS AT LAW

What Should Companies Do?

Bethesda AFCEA Chapter

- Perform a self-assessment and gap analysis to identify areas needing improvement prior to approaching insurers
- Develop an enterprise-wide action plan based on the Cybersecurity Framework (enterprise risk management)
- Develop and regularly test a cybersecurity incident response plan
- Hire outside consultants to provide objective vulnerability assessments
- Hire outside counsel first, and have them engage all other contractors and conduct all internal investigations to ensure attorney-client privilege
- Consider the SAFETY Act

What Should Companies Do?

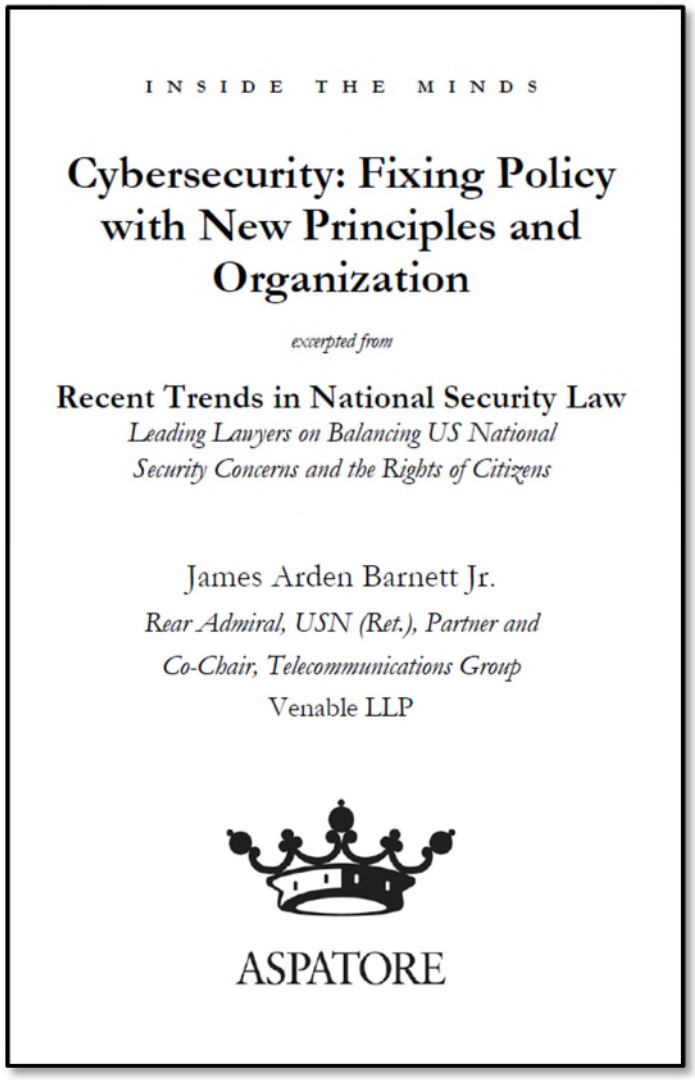
- Elevating
  - Boardroom responsibility; Enterprise-wide approach
- Understanding
  - Identify data assets
  - Review organizational governance
- Securing
  - Vendor controls
  - Penetration testing and other measures
  - Incident Response Plan

VENABLE®
ATTORNEYS AT LAW

What Should We Do About Cybersecurity Policy?

What is the Government's Proper Role?

Bethesda AFCEA Chapter



INSIDE THE MINDS

Cybersecurity: Fixing Policy with New Principles and Organization

excerpted from

Recent Trends in National Security Law

Leading Lawyers on Balancing US National Security Concerns and the Rights of Citizens

James Arden Barnett Jr.

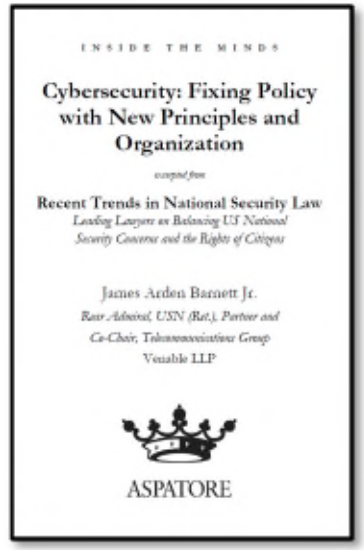
Rear Admiral, USN (Ret.), Partner and Co-Chair, Telecommunications Group

Venable LLP

ASPATORE

What Should We Do About Cybersecurity Policy?

What is the Government's Proper Role?



Principles for addressing cyber security policy include the following:

- Cyber space should remain a place for innovation and free expression.
- Privacy must be protected in cyber space.
- Security in cyber space and the protection of the Internet is the responsibility of the private sector.
- The primary function of the government should be to support and aid the private sector in providing cybersecurity.
- Where the market will not provide adequate cybersecurity, the government should provide incentives and regulations to raise the bar.

Questions?

Contact Information

James Arden "Jamie" Barnett, Jr., Esq.
Rear Admiral USN (Ret)
Co-Chair Telecom/Cybersecurity Practice
jbarnett@venable.com
(202) 344-4695