# Promoting Global Frameworks and Norms to Enhance Cybersecurity

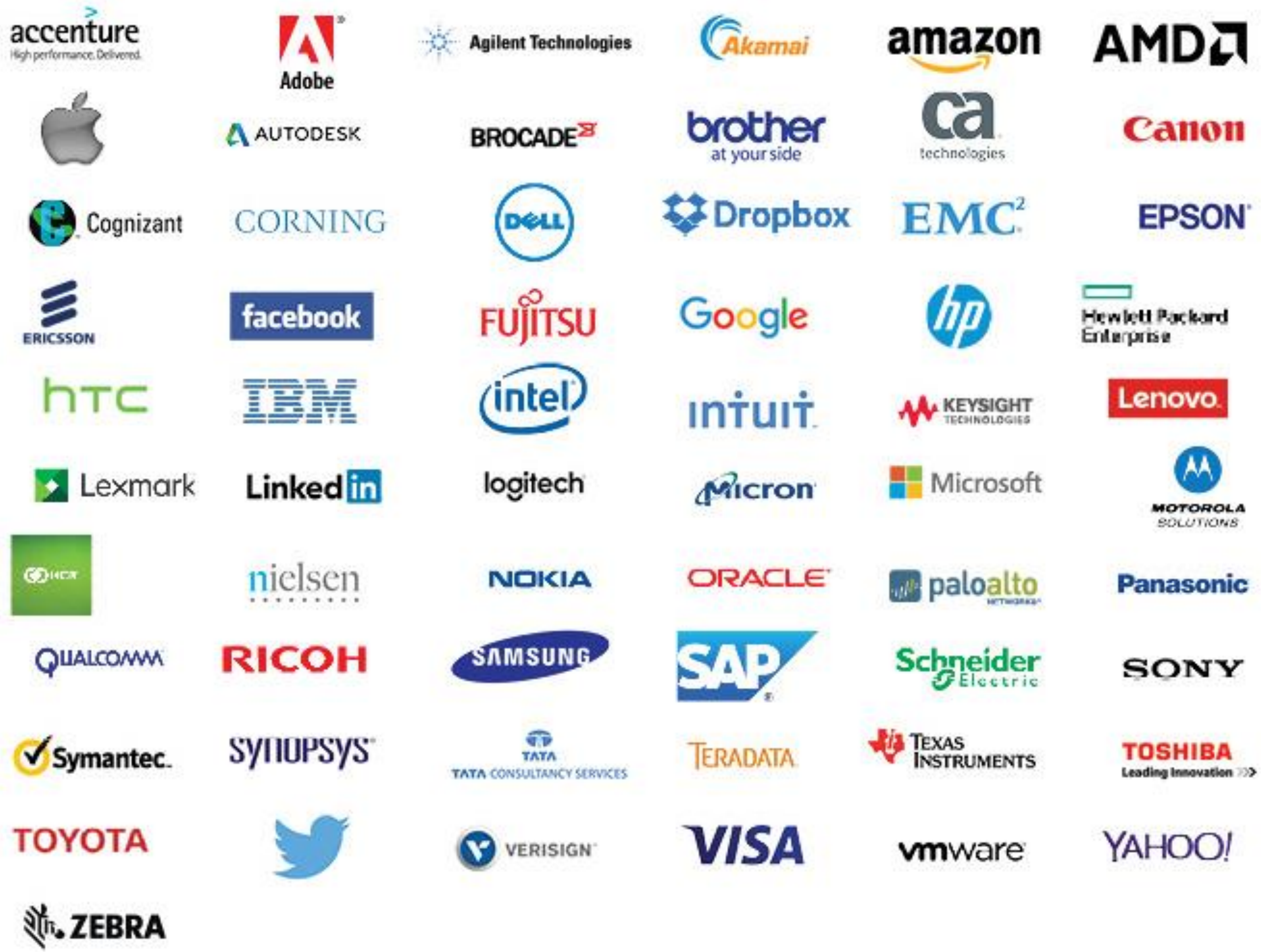
**John S. Miller**

Vice President for Global Policy and Law,
Cybersecurity and Privacy

18 April 2016

# About ITI

- The Information Technology Industry Council (ITI) is the premier policy and advocacy organization for the world's leading innovation companies.
- We advocate for global policies that advance industry leadership, open access to new and emerging markets, promote e-commerce expansion, drive sustainability and efficiency, protect consumer choice, and enhance worldwide competitiveness of our member companies.

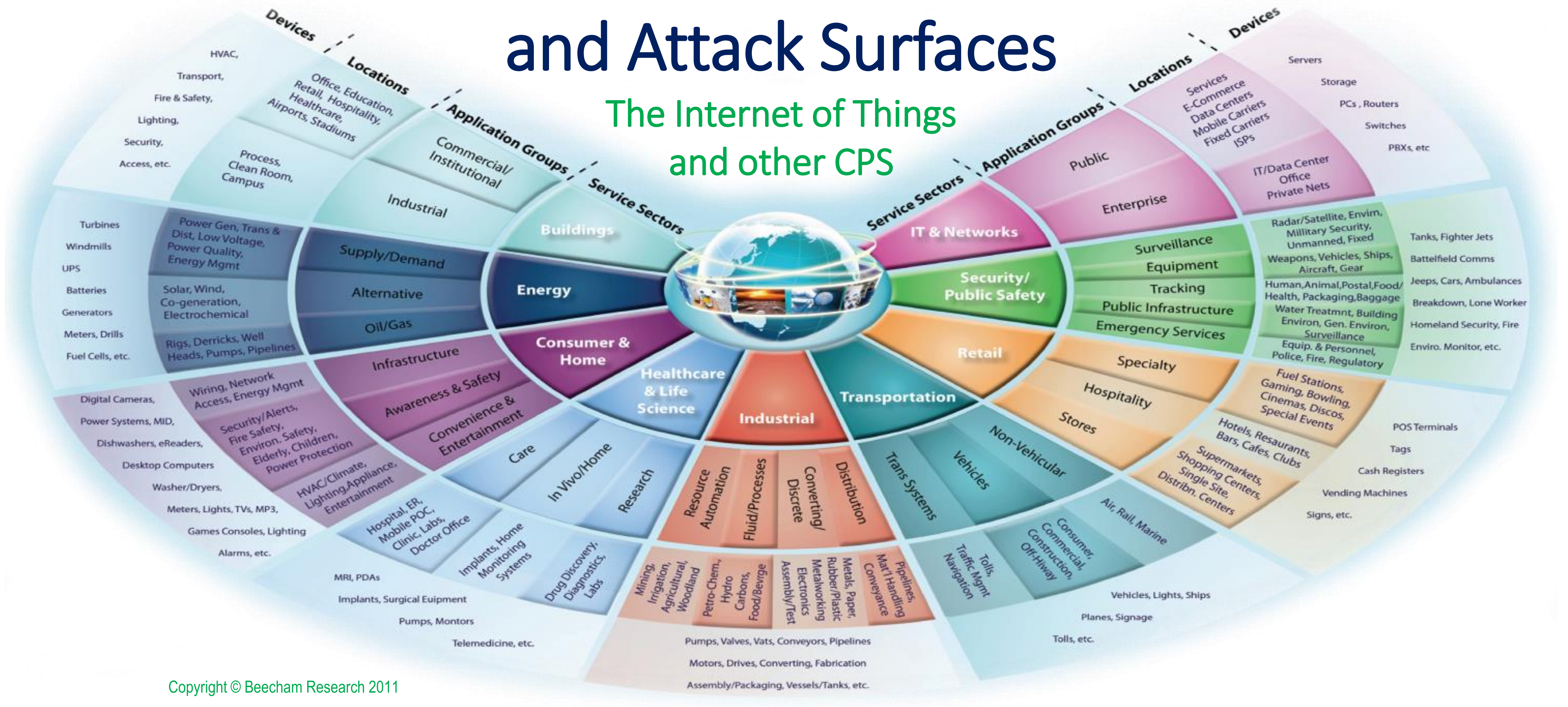

accenture
High performance. Delivered.
Adobe
Agilent Technologies
Akamai
amazon
AMD
AUTODESK
BROCADE
brother
at your side
ca
technologies
Canon
Cognizant
CORNING
DELL
Dropbox
EMC²
EPSON
ERICSSON
facebook
FUJITSU
Google
hp
Hewlett Packard Enterprise
htc
IBM
intel
intuit
KEYSIGHT TECHNOLOGIES
Lenovo
Lexmark
LinkedIn
logitech
Micron
Microsoft
MOTOROLA SOLUTIONS
NCR
nielsen
NOKIA
ORACLE
paloalto NETWORKS
Panasonic
QUALCOMM
RICOH
SAMSUNG
SAP
Schneider Electric
SONY
Symantec.
SYNOPSYS
TATA
TATA CONSULTANCY SERVICES
TERADATA
TEXAS INSTRUMENTS
TOSHIBA
Leading Innovation
TOYOTA
VERISIGN
VISA
vmware
YAHOO!
ZEBRA

# ITI's Work on Cybersecurity

- ITI's work and perspective on cybersecurity is global
  - ITI engages in DC and in capitals around the world (Beijing, Delhi, Brussels, Seoul, Tokyo …)
- Principles: To be effective, efforts to improve cybersecurity should:
  - Leverage public-private partnerships, build upon existing initiatives & resource commitments
  - Reflect the borderless, interconnected, and global nature of today's cyber environment
  - Be able to adapt rapidly to emerging threats, technologies, and business models
  - Be grounded in effective risk management
  - Focus on raising public awareness
  - More directly focus on bad actors and their threats

# New World of Digital Footprints and Attack Surfaces

## The Internet of Things and other CPS



Service Sectors
Application Groups
Locations
Devices

Buildings
Commercial/ Institutional
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Industrial
Process, Clean Room, Campus
HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.

Energy
Supply/Demand
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Alternative
Solar, Wind, Co-generation, Electrochemical
Oil/Gas
Rigs, Derricks, Well Heads, Pumps, Pipelines
Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.

Consumer & Home
Infrastructure
Wiring, Network Access, Energy Mgmt
Awareness & Safety
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
Convenience & Entertainment
HVAC/Climate, Lighting,Appliance, Entertainment
Digital Cameras, Power Systems, MID, Dishwashers, eReaders, Desktop Computers, Washer/Dryers, Meters, Lights, TVs, MP3, Games Consoles, Lighting, Alarms, etc.

Healthcare & Life Science
Care
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
In Vivo/Home
Implants, Home Monitoring Systems
Research
Drug Discovery, Diagnostics, Labs
MRI, PDAs, Implants, Surgical Euipment, Pumps, Montors, Telemedicine, etc.

Industrial
Resource Automation
Mining, Irrigation, Agricultural, Woodland
Fluid/Processes
Petro-Chem, Hydro Carbons, Food/Bevrge
Converting/ Discrete
Assembly/Test, Electronics, Metalworking, Rubber/Plastic, Metals, Paper,
Distribution
Pipelines, Mat'l Handling Conveyance
Pumps, Valves, Vats, Conveyors, Pipelines, Motors, Drives, Converting, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.

Transportation
Trans Systems
Tolls, Traffic Mgmt, Navigation
Vehicles
Consumer, Commercial, Construction, Off-Hiway
Non-Vehicular
Air, Rail, Marine
Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.

Retail
Specialty
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hospitality
Hotels, Resaurants, Bars, Cafes, Clubs
Stores
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.

Security/ Public Safety
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Radar/Satellite, Envim, Millitary Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Tanks, Fighter Jets, Battlefield Comms, Jeeps, Cars, Ambulances, Breakdown, Lone Worker, Homeland Security, Fire, Enviro. Monitor, etc.

IT & Networks
Public
Services, E-Commerce, Data Centers, Mobile Carriers, Fixed Carriers, ISPs
Enterprise
IT/Data Center, Office, Private Nets
Servers, Storage, PCs , Routers, Switches, PBXs, etc

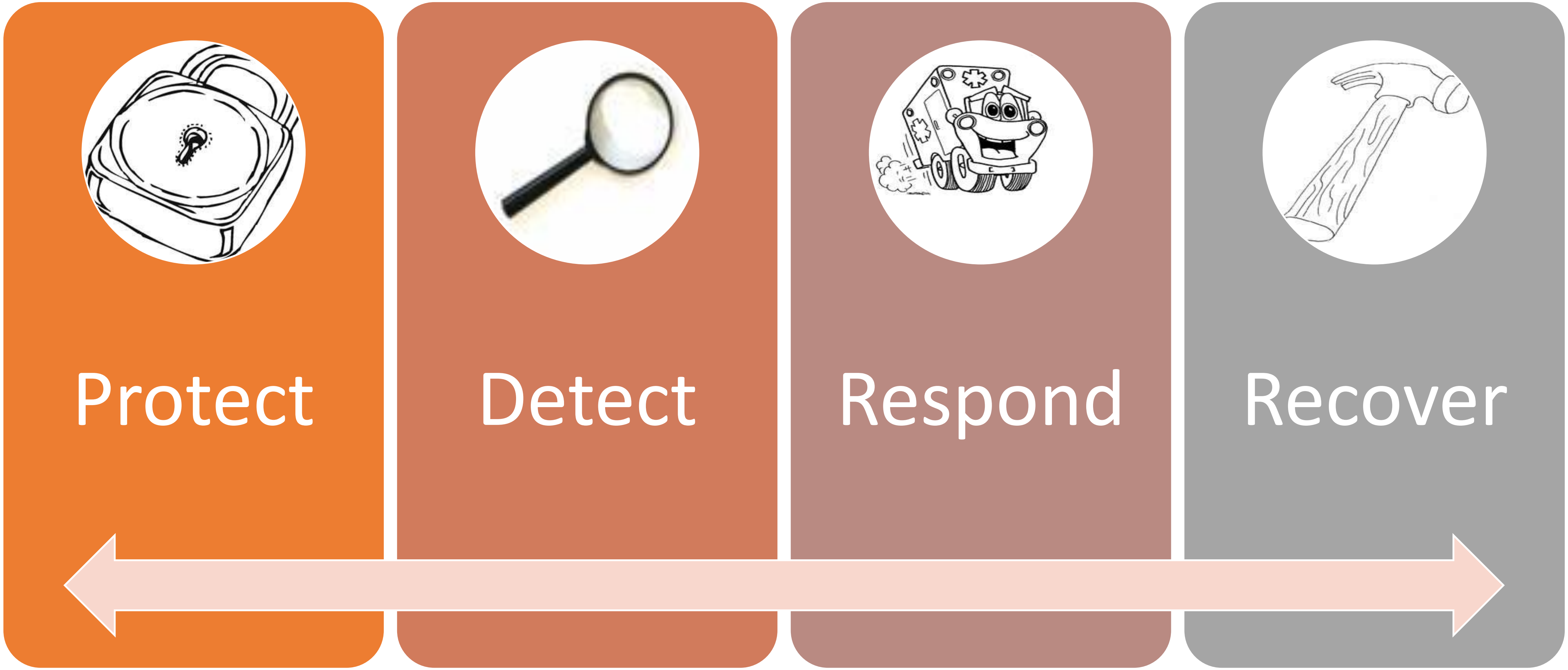
# Cybersecurity Framework

## Building a Common Language to Manage Risk

# What is the Cybersecurity Framework?

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity signed by US president in 2013.
- NIST designated as "convener" to work with industry via a public/private partnership.
- Industry identified consensus best practices, and NIST compiled a set of known, publicly vetted mostly international standards that can be applied to identify, protect from, detect, respond to, and recover from risks.
- White House Statement: "Enables organizations -- regardless of size, degree of cybersecurity risk, or cybersecurity sophistication -- to apply the principles and best-practices of risk management to improving the security and resilience of critical infrastructure."
- Framework does not dictate specific technologies, measures, or outcomes – not prescriptive
- Framework establishes a common language for organizations to evaluate their cybersecurity posture and to identify and prioritize opportunities to improve it.
- Framework is designed to be adaptable to organizations of different types and sizes & can be customized to an individual organization depending on its risk profile, resources, and needs.
- Framework is a voluntary template for organizations to use in developing better security programs.

Cyber Framework Published February 2014



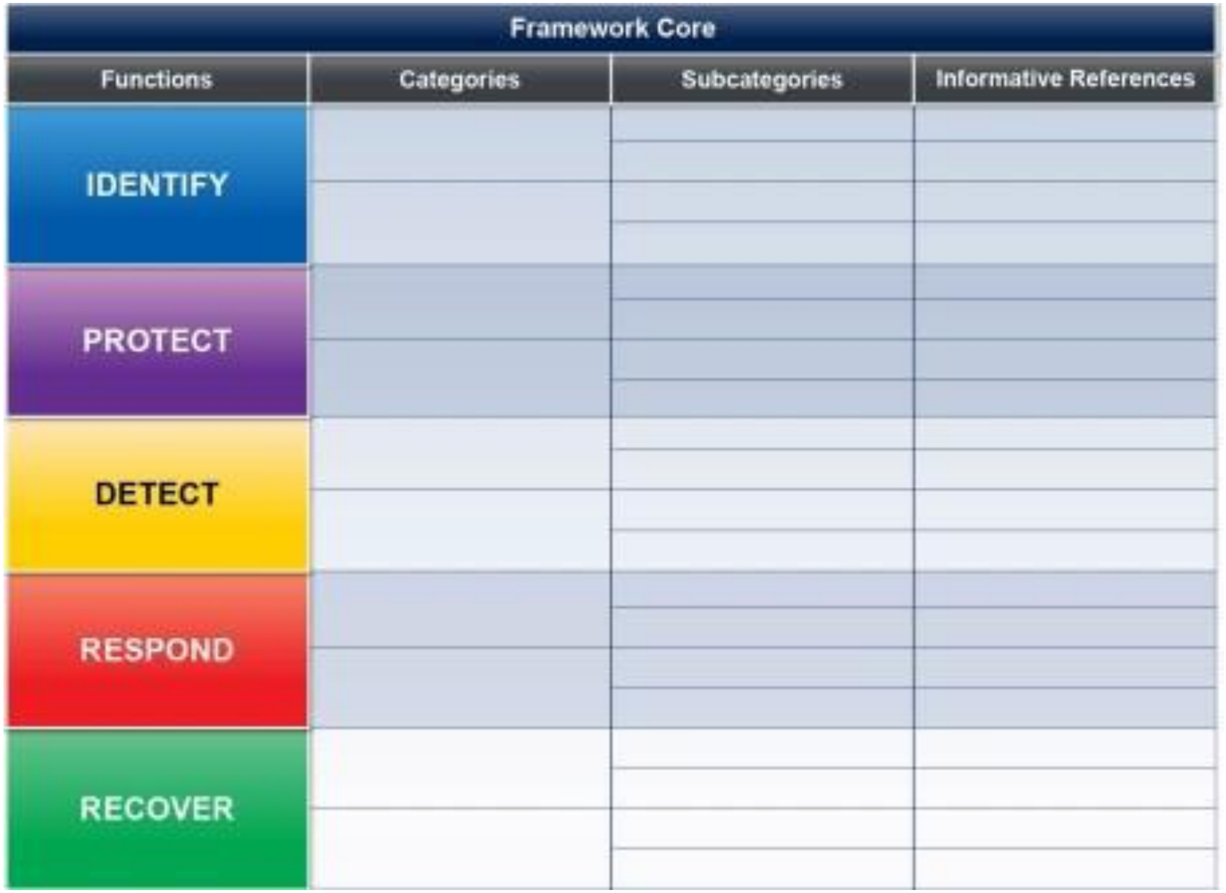
Protect

Detect

Respond

Recover

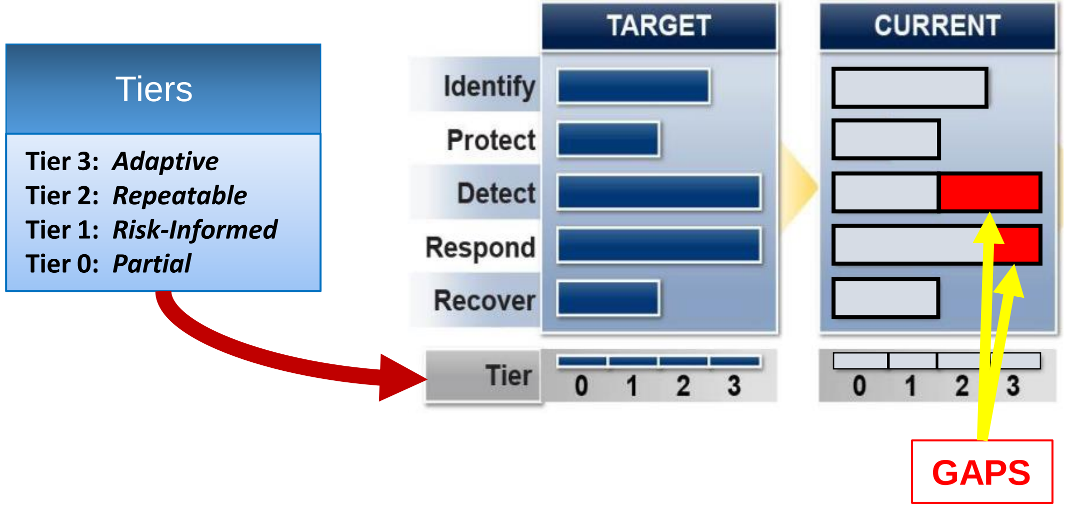
# Cybersecurity Framework: A Risk Management Framework and Maturity Model



| Framework Core | | | |
|---|---|---|---|
| Functions | Categories | Subcategories | Informative References |
| IDENTIFY | | | |
| PROTECT | | | |
| DETECT | | | |
| RESPOND | | | |
| RECOVER | | | |

*Risks are assessed by Function Area with the ability to examine risks granularly through Categories/Sub Categories enumerations*

PROFILE EXAMPLE: Energy Sector



Tiers

Tier 3: *Adaptive*
Tier 2: *Repeatable*
Tier 1: *Risk-Informed*
Tier 0: *Partial*

***Tiers and Maturity Levels***

1. *Organizations set Target Maturity Levels to match their Risk Tolerance*
2. *Organizations examine their controls and assess gaps against Targets*

# Building a Common Language

- The Framework provides a common language and is an important risk management tool to improve cybersecurity
- The Framework's value for organizations of all types
  - Communications – enabling conversations amongst internal stakeholders
  - Internal systems – across enterprises of all sizes
  - Products – across products, with global customers
  - Supply chain – across ecosystem, with global suppliers
- The Framework's value as a global policy tool
  - Provides a global language across governments as well
  - Framework grounded in international standards
  - Approach encourages public-private partnership

# Cybersecurity Framework as a Global Policy Tool

- Framework approach = a counterweight to overly prescriptive approaches
  - Pulling environment away from compliance-based security, toward risk management
- We have seen a cyber policy sea change in the U.S.
  - Admin. abandoned top-down regulatory approach in favor of voluntary, risk-management based approach embodied in the Framework
  - Federal government agencies, states embracing as well as companies
  - Industry – multiple sectors aligned, working together
- Framework approach is gaining traction globally
  - Italy launched "National Framework" in Feb. 2016
  - Interest in other geographies growing

"MAN IS A TOOL-USING ANIMAL. WITHOUT TOOLS HE IS NOTHING, WITH TOOLS HE IS ALL."
THOMAS CARLYLE
Lifehack Quotes
po'licey
membe
the
pol·icy
statement of i

# Promoting Cybersecurity Norms

## Through Bilateral and Multilateral Commitments

# Momentum Building Around Cybersecurity Norms

- UN Group of Governmental Experts Report – 2015
- Bilateral Commitments – U.S. and China  2015
- G20 Affirms Norms at Turkey Leaders Summit – 2015
- U.S. Reaffirms Commitment to Norms in CNAP– 2016
- Joint ICT Recommendations to G7 – 2016
- G7, G20 and Beyond 2016

# What are Cybersecurity Norms?

- Agreed Multilateral and Bilateral Commitments around Cybersecurity Norms
  - Applicability of International law to cyberspace
  - Abiding by norms of responsible state behavior in cyberspace
  - States should not conduct cyber-enabled theft of IP for commercial advantage
  - Establishing high-level dialogues to fight cybercrime
  - Welcoming UN Experts report
- Cybersecurity Norms under Consideration - Examples
  - Promoting greater openness, interconnectivity and interoperability as essential to a stable, secure and accessible global ICT environment
  - Promoting international cooperation to increase ICT stability and security
  - Preventing attacks on civilian critical infrastructure
  - Encouraging responsible vulnerability disclosure and sharing
  - Supporting CERTs

# THANK YOU!

John S. Miller

jmiller@itic.org

+1-202-626-5731