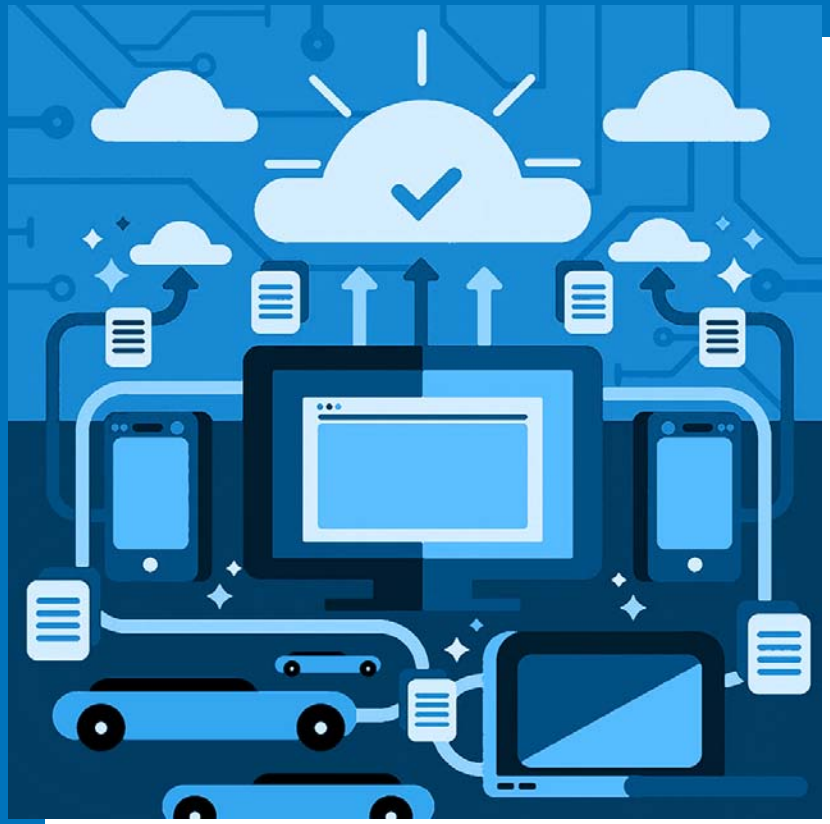
# BREAKTHROUGH GROUP REPORTS

## PART I

#EWIcyber



# Resilient Cities and the Internet of Things

#EWIcyber

## Substantive Discussion and Results

- Uncertainty around city resiliency
- Interaction and tradeoffs between security and privacy
- The growing ecosystem and interdependencies

#EWIcyber

## Breakthrough Group Next Steps

- Scope of smart cities, safe cities, and IoT (IIoT) – Altabef's 4 dimensions
- Governance frameworks and use cases (best practices)
- Understanding the emerging IoT ecosystem
- Cyber resilience in urban environments of today
- Explore potential partnership opportunities

#EWIcyber

# Systemic Risk and Cyber Insurance

#EWIcyber

# Substantive Discussion and Results

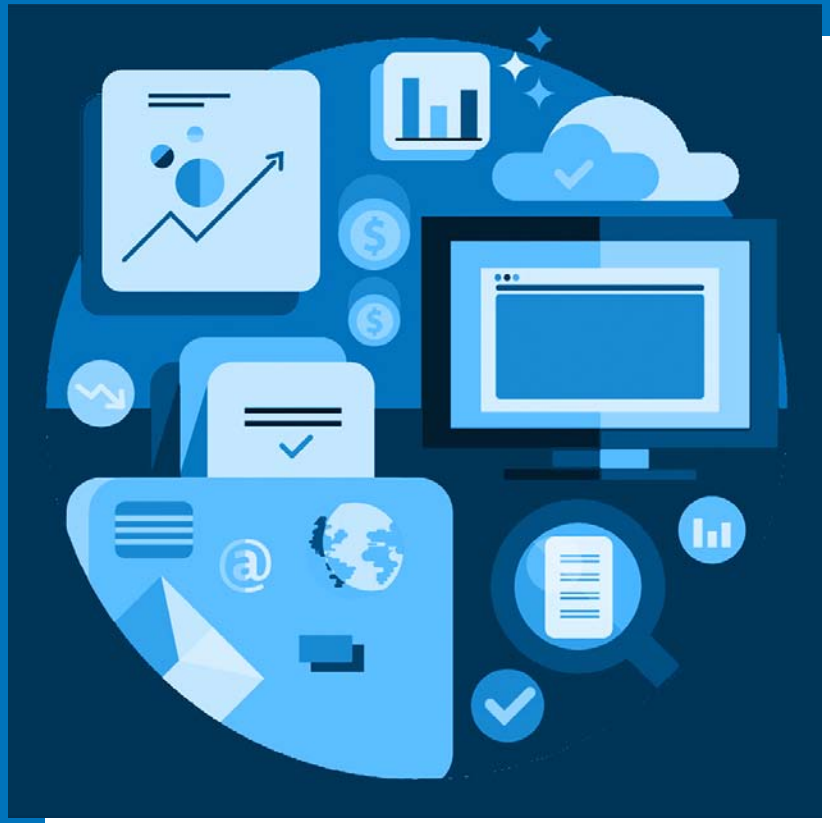
- Systemic cyber risk is hard to define, but must focus on key components that lead to cascading failures internationally and encourage harmonized prescriptions
- The insurance industry is thinking more about predictive modeling to measure its cyber risk, which can help inform resilience efforts
- Components that present systemic risks, can also be used to control and mitigate this risk
- Industry partners should drive effort to identify these components across sectors of Finance, Energy, IT, Health, Transportation, and Communications

#EWIcyber

# Breakthrough Group Next Steps

- Agree on a common understanding of systemic risk and how to frame it
- Leverage other EWI working groups to help inform components that present most risk and opportunity for mitigation
- Engage insurance industry to bring together multiple modeling stakeholders to help quantify systemic risk impact
- Prioritize systemic risk areas based on modeling of largest impact
- Informed by these modeling efforts, provide international policy makers with most critical areas to affect positive change

#EWIcyber



# Secure ICT Products and Services

#EWIcyber

**BG Co-Leads:**
Angela McKay, Microsoft – Andy Purdy, Huawei - Sally Long, The Open Group

**BG Objective:**
To enhance cybersecurity for governments and enterprises globally by enabling the *availability* and *use* of more secure ICT products and services.

**Global ICT Challenge:**
- ICT Marketplace thrives because of global economy but => introduces cyber risks
- Customers concerned about cyber risks but => don't know what to ask of suppliers
- Uncertainty and mistrust => disparate local requirements => trade barriers

**#EWIcyber**

## BG Approach:

- Develop Buyer's Guide as initial vehicle to address challenges
- 1.0 Released Sept 2016: Increases awareness of the landscape – and provides guidance on what buyers should be asking of their suppliers
- Appendices - references cyber and supply chain standards and conformance programs – 100 Questions to ask of suppliers – Provides feedback form

## This Week BG Sessions focused on Buyer's Guide – To solicit feedback

- Reinforced the need for such a guide and for the messaging of the guide
- Appreciated the focus on international standards and conformance/assurance
- Evolution of the Guide is important
- Need to increase awareness by expanding outreach efforts

**#EWIcyber**

# Breakthrough Group Next Steps

Evolve the Guide:

- Improve framing and positioning (audience, expectation, how to use guide)
- Add sub-section on various roles involved in buyer-supplier ecosystem
- Provide supplemental material => 2 case studies: role-based (e.g., CFO or procurement officer) and vertical-market based (e.g., IoT segment). Case studies linked from the Guide
- Consider consolidating 100 questions to increase scalability – increase importance of questions around international standards to improve scalability
- Evaluate whether we need to enhance Cyber Security Framework (CSF) focus within the Guide
- Provide collective comments to CSF 1.1 by April 10 – recommend additional informative references related to supply chain standards
- Timeline and actions for deliverables: Actions and milestones for interim work depends on number of participants to do the work – to be fleshed out in next couple of weeks. Release of next version of the Guide may be dependent on external events (e.g. Publication of CSF 1.1)

# Breakthrough Group Next Steps

Increase Awareness of the Guide:

- Webinars or interviews that promote the BG initiative and the Guide
- Work with these targeted organizations through small meetings or large events:
  - NIST, APEC, G20, ITU, OAS, Bay Area Council, Financial Sector, Center for International Governance Innovation, GFCE (note: annual meeting May 31 in Brussels to plan 2017 work agenda) Security Alliance, FAR/DFAR (simply to increase awareness)
  - Target Outreach list (above) is dynamic - to be added to and Prioritized
  - Increase focus on the fiduciary due-diligence responsibility of organizations to address cybersecurity risk including third-party risk (such as supply chain risk), by working with organizations like the American and International Bar Associations.

# BREAKTHROUGH GROUP REPORTS PART II

#EWIcyber

# Ubiquitous Encryption and Lawful Government Access

#EWIcyber

# Substantive Discussion and Results

- Encryption debate has been happening for more than 20 years
- Strong encryption continues to become more widely available, notably in OTT and end points
- Law enforcement is finding that they are increasingly unable to access communications or devices due to full disc and end-to-end encryption
- There is a lack of trust between law enforcement and the tech industry, technologists, and civil society

[See "Keys Under Doormats," "Don't Panic," CSIS, and "Congressional Encryption Working Group"]

# Breakthrough Group Next Steps

- There is a need to soften rhetoric and listen to the concerns of the other side
- Focus on measurement and quantification of risks and needs of LEA (e.g. number of cases that required access to devices, how different solutions increase overall risk, etc.)
- Identify common vocabulary (backdoor, front door, side door)
- Break the problem into smaller components (e2e vs device vs cloud)
- Provide law enforcement with better access to resources and tools (new sources of data)
- Develop public awareness campaigns aimed at raising awareness about risks in the connected world being similar to risks in the physical world

#EWIcyber

# Promoting Norms of Responsible Behavior in Cyberspace

#EWIcyber

## Substantive Discussion and Results

- Remain conscious of role and goal of norms
- In capacity building, align efforts with concrete needs
- Boundaries of 'critical infrastructure' not always clear
- Be aware of existing norms when building new ones

#EWIcyber

## Breakthrough Group Next Steps

- Operationalize common interests and common risks
- Develop metrics, asset mapping for capacity building
- Support and integrate GCSC and EWI initiatives
- Map existing norms: domestic, international, industry

#EWIcyber

# BREAKTHROUGH GROUP REPORTS

#EWIcyber