Partnering for Cyber Resilience

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

June 2013 Newsletter

Welcome back as we launch Phase II

Dear Members of the Partnership for Cyber Resilience,

Thank you for your continued support, as we launch Phase II and lay the groundwork for Phase III of the Partnership.

Over the past year, we have grown our base to boast 97 companies and governments across 16 industries and 23 countries. Consistent with this effort, our network has worked tirelessly to drive societal change and we thank you all for your efforts in developing leadership, awareness and understanding.

For 2013, in addition to continuing to promote the *Principles*, we aim to help foster broad collaboration and action. Specifically, over the course of this year, we will seek to engage all members in in-depth discussion around 3 areas: information sharing; governance and policy development process, and critical infrastructure protection. We also invite PCR member to contribute your thought leadership to developing a global scenario of the future cyber landscape and producing a financially-driven economic model. The Forum aims to leverage its network to help develop a list of key actions that individual organizations can take in the near-term to mitigate the threat from cyber attacks.

Throughout the year, we will also seek to lay the foundation for independent taskforces by providing our partners with the tools and resources to form individual cohorts centered on particular topics of interest. The Forum will provide various support levers, as we transition to Phase III, a full set of community driven initiatives.

As always, we look forward to working you and look forward to an exciting year,

Colombia is having national discussions on Cyber Security Strategies

On March 14, the World Economic Forum took part in a national discussion on cyber security strategy for Colombia. We joined various officials from across the nation's government and cyber security officials including Minister of ICT, Diego Molano Vega. Minister Vega has been a strong supporter of the Principles and recognized that cyber security poses an immediate threat.

The Minister stressed the importance of the public and private sectors to take necessary measures to fulfil the at minimum basic security requirements in the as they relate to sensitive information.

It was the opinion of many during the discussion that the general population is not yet aware of the threats to the cyber ecosystem and that within Colombia, for example, an awareness campaign has been long overdue.

It was also stressed that an international document helping coordinate the actions in case of a cyber attack would be beneficial to all .

Along these lines, officials from Colombia are interested in learning more from the experiences of other countries as it works to create its new country -level strategies.

Mirroring our key topics for 2013, the group touched on the ideas of information sharing and critical infrastructure.

Relating to information sharing, a strong push was made for the need to report cyber attacks, which will help coordinate efforts and produce better responses. Minister Vega noted that if companies do not anticipate cyber attacks, they will continue to experience problems. The Minister highlighted that although 80% of Colombian critical infrastructure is private, there is still no country wide understating of which components are critical.

On critical infrastructure protection, the Minister highlighted that although 80% of Colombian critical infrastructure is private, there is still no a country wide understating of which components are critical.

In line with best practices, Colombia is now moving towards using more biometrical information as a way to secure authentication mechanisms but will continue to need to work to make sure that the vulnerabilities associated.

Overall, Colombia is looking for effective PPP mechanisms to help address cyber threats. Through this development process, it is aiming to be actively involved in the international debate on the topic with specific focuses on information sharing, securing critical infrastructure.

Power brainstorming on the key challenges and opportunities from the Japanese perspective

In late April, representatives from government, business and academia convened in Tokyo for a small, high-level early stage brain-storming on what the key challenges and opportunities were within these domains from a Japanese perspective.

Despite strong consensus on the importance of the issues, early comments revealed a broad range of frameworks through which different organizations approach the issues at hand – including economic, technical, policy and diplomatic lenses. Nevertheless, a number of key themes emerged from the dialogue:

Providing the foundations for an open, secure and resilient internet is critical to economic growth

Awareness of the real and potential impact of cyber failures is growing

A common framework is required to support clear understanding of roles and responsibilities, e.g. between companies and different government agencies, and to avoid fragmentation

Not everyone understands nature of risks: as everything becomes connected, human error can be as dangerous as intentional attack

Information Sharing

Japan is a recognized leader in collaborative efforts to tackle cyber risks. Nevertheless, several barriers remain. At the highest level, and in common with other regions, the biggest change that participants felt necessary was one of culture. Despite great progress in this domain, for many organizations there may still be significant reputational concerns around revealing breaches.

In response to these challenges, workshop participants developed some concrete recommendations. In particular, building upon an recent information sharing initiative which has demonstrated good success. A model was proposed where the government acts as the convenor for an information sharing centre/group but does not run it exclusively. Rather, it is run by a multi-stakeholder group with representation from the variety of parties involved. Anonymous centralized NDAs, along with standard protocols for what information is shared and how, provide the requisite levels of assurance to participating organizations. While this currently runs across five industries, it was proposed that it could be broadened out across more verticals, and the model could also be shared with other jurisdictions, perhaps through ASEAN for example.

Critical Infrastructure & Systems in a Digitally Connected Society

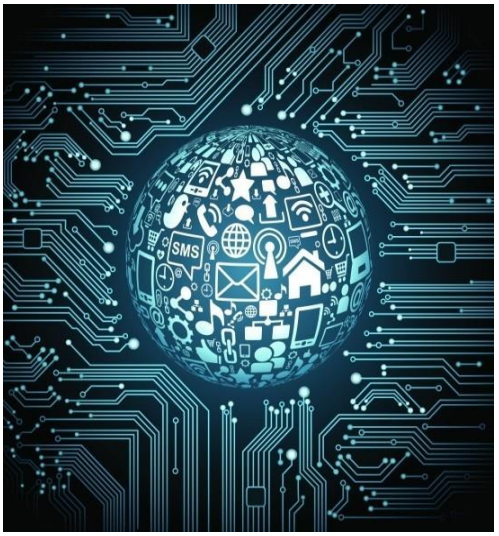
In contrast, some previous discussions elsewhere, most participants felt relatively comfortable with the existing national definitions of critical infrastructure. However, this was the one area which emerged as being the key priority among the experts, as a number of barriers exist to operationalize the guidelines which have been laid out at a national level. In particular, there remain assurance issues in the absence of an independent mechanism to verify to what extent organizations and industries have actually implemented the guidelines provided.

As such, many organizations feel that they bear undefined third party risks through their supply chains.

Participants provided a number of concrete proposals to make progress here, specifically the adoption go standardised benchmarking and the provision of independent accreditation. Furthermore, the adoption of these tools to measure risks and verify mitigation actions would provide the foundations for an effective insurance market to emerge. This has been seen elsewhere, and provides market incentives to organizations to move beyond a compliant mind-set to a risk-mitigation, competitive mind-set.

Role of the Public Sector

A common theme throughout these discussions is the role of the government. Two key points emerged, which are consistent with conversations held in other regions. Firstly, government is not a single entity. This can provide challenges both within the public sector to coordinate and for other stakeholders who wish to understand the relative roles and responsibilities of different departments and agencies in a complex, interdependent set of issues. Again, while great strides have been made in this area in Japan, this ever-evolving landscape means that this is an on-going dialogue rather than a one-off exercise. A second common theme was a growing recognition that in many areas, the most powerful role that government could play is not just as policy-maker or regulator, but as an enabler. Many of the concrete proposals put forward involve a variety of private, public and other stakeholders working together in a trusted environment – and government sits in an ideal position to provide the enabling conditions to support such broad collaboration.



Exploring the potential for a CDC for Cyber in San Francisco

Background

At the 2013 Annual meeting, a group of group of ICT industry executives and policymakers proposed the creation of a mechanism to share best practices and information about cyber threats. In May, the group reconvened to assess the feasibility of the approach, outline the main barriers, and propose the next steps in moving towards better information sharing and monitoring of cyber threats.

During their discussion, the group focused on two parts: the first part were reasons why a "CDC for Cyber" is not feasible, the second was aimed at addressing these concerns and finding a common ground to suggest models for a functioning and effective cyber CDC globally.

Why might "CDC for Cyber" not work?

Within the discussion, participants identified a few key concerns as to why a CDC for Cyber may not be an option. A few of the perspectives were as follows:

- *Legal and regulatory issues*: sharing of certain information may be unlawful under current regulations
- *Severity*: Level of breaches may not constitute a serious issue in terms of fiscal, brand or other impact
- *Centralized approach is counter intuitive*: by centralizing all the materials, we have would make the information an even larger target
- *Willingness to participate*: CEOs would be unwilling to contribute sensitive or proprietary information that could be used by competitors
- *Potentially lower value*: may not have the ability to analysis the data or provide meaningful outputs because of the type and completeness of the data presented
- *Lack of responsible agency:* unclear who would be responsible for maintaining and acting upon information provided
- *Free rider issue:* how would you determine who is eligible to participate and what happens if people fail to contribute information

Based on these identified issues, amongst others, the taskforce then worked to identify potential resolutions to the challenges.

What models of information sharing can work?

- The second session aimed at addressing existing concerns and finding areas for common action among various stakeholders.
    - Trusted information sharing systems: a potential match making approach where each participant has "skin in the game" in a very controlled environment and on a voluntary and private basis
    - Sustainable economic approaches: create scalability to make space for additional businesses and have a pooled fund to purchase additional assets/tools/resources

Based on these decisions, the group identified that good places to start would be reporting the basics of attacks rather than specific and creating a narrow focus only where people need to share information.

Additionally, the group will specific work to facilitate peer-to-peer networks and knowledge exchanges, encourage CEOs to report attacks, advise on improving the legislation on liability in sharing cyber threat information, and develop a preliminary concept of information sharing with the aim of presenting the information at the Annual meeting in Davos 2014 amongst other actions.

Ensuring Africa's promise in a digitally connected world

With so much of Africa's promise linked to digital connectivity, ensuring continued trust in the digital environment continues to be a critical linchpin in driving and accelerating inclusive social and economic innovation, transformation, investment, growth and competitiveness. From a global perspective we are only as strong as our weakest link, so in that frame, all states have an incentive to ensure that each is equipped to be responsible in an evermore digital 21st century.

Through a series of sessions, participants began to define the basic capabilities that a country should have in terms of cyber resilience.
Participants were asked to engage on two questions:

- What are the basic cyber resilient capabilities every country should have?
- What institutions are required to deliver on these capabilities and what is the role of the private, public and civil society sectors?

From these conversations a clear framework emerged. Participants called for a clear legislative environment for cyber crime with law enforcement capabilities and trained resources throughout the criminal justice chain to support legislation. They also championed education and public awareness campaign and best practice sharing platforms to ensure transparency and dissemination of ideas. Finally, a call for national security frameworks and dedicated strategies embedded into each Ministry as well as a coordinating agency to effectively manage rising issues.

Additionally, there was an aggregation of innovative examples of types of mechanisms required to deliver on these (e.g. countries appointing a Chief Security Officer, developing a multi-stakeholder network with the private sector and civil society). The results will feed into dialogue to create a best practices guide for governments, a potential fund to provide advisory services and the development of a measurement index.

Bridging the Digital Divide in Mexico

The World Economic Forum joined the Organization of American States (OAS) and representatives from four companies at the Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) as part of World Internet Day in Mexico City, Mexico on 16 May.

Fernando Gurrola Alvarez, President of the Mexican Internet Association was joined by Embassador Anibal Quinone, Deputy from OEA in Latin America, Miguel Calderon, Vice President from Telefonica Mexico (as a representative of Francisco Gil Díaz, President of Telefonica), Juan Alberto Gonzalez Esparza, President from Microsoft Mexico, and Ciro Humberto Ortiz Estrada, National Security Commission, in signing the Principles for Cyber Resiliency.

As part of its mission to accelerate the development and evolution of the internet, the Association Mexicana de Internet (AMIPCI) holds an annual celebration every World Internet Day in Mexico. As part of this year's celebration, the AMIPCI, in coordination with several other local and international organizations hosted a two day event with sessions on public policy, interactive advertising, digital entrepreneurship, and society and accountability.

Calendar of Events 2013

Following the CDC for Cyber event in May, two key events are coming up for the Partnering for Cyber Resilience initiative.

We are looking forward to the World Economic Forum Advisory Meeting on Global Risks on June 11-12th.

Secondly, the OAS will host a workshop on Cyber Security and its Implications on the Economy and the Financial Sector on June 26th.

The calendar below shows a selection of opportunities for the Partnership to grow or develop guidelines for policy and law enforcement communities. If you want to add your event to the calendar, please inform the team. The calendar is updated regularly and available for download here.

*Planned

	May	June	July	August	September	October	November	December	January
Forum-led events		**Global Risks Workshop** Geneva 11-12 June			**Annual Meeting of New Champions** Dalian, China 13-16 Sept		***Americas Regional Summit** North America Early Nov ***Asia Regional Summit** Europe Early Nov. ***EMEA Regional Summit** Europe Early Nov.		**Annual Meeting** Davos 22-26 Jan.
Project Dialogues			**BlackHat USA** Las Vegas, USA July 30 (TBC)		***High-tech/ Manufacturing Dialogue** North America TBC ***Financial Services Dialogue** North America TBC ***Infrastructure, Resouces, and Utilities Dialogue** North America TBC	***Advanced Industries Dialogue** EU/ Asia TBC ***Healthcare Dialogue** North America TBC	**The Grand Conference** Amsterdam, Netherlands November 5		
Community-led events	**CDC for Cyber** San Francisco 14 May	**OAS Workshop** D.C. 26 June				**Cyberspace Summit** Korea October **OAS Workshop** Chile Early Oct.			

Our Partners for Cyber Resilience

Agriculture, Food & Beverage

Automotive

Aviation & Travel

Banking & Capital Markets

Chemicals

Energy Utilities & Technology

Government & Not-for-Profit

IT

Insurance & Asset Management

Media, Entertainment & Information

Mining & Metals

Multi-Industry

Private Investors

Professional Services

Retail & Consumer Goods

Supply Chain & Transport

Telecommunications

Is your logo incorrect or missing? Please tell the team.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is tied to no political, partisan or national interests.

Partnering for Cyber Resilience

The Partnering for Cyber Resilience initiative seeks to build a community of private and public sector leaders who join forces to deal with the new risks and responsibilities of the hyperconnected world.

Together they support the Principles for Cyber Resilience, leading cyber risk management for their organizations, and with the public sector, for society as a whole.

Sincere thanks are extended to the experts who contributed their unique insights to this initiative.

For the latest information on the Partnering for Cyber Resilience initiative, please visit: weforum.org/cyber

Contact:

Elena Kvochko
Partnership for Cyber Resilience Lead

cyberresilience@weforum.org