Partnering for Cyber Resilience

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

February 2013 Newsletter – Davos Special Edition

World Economic Forum Annual Meeting 2013, Davos-Klosters

Friday 25 January 2013 marked the first anniversary of the Partnering for Cyber Resilience (PCR) initiative. Since its launch at Davos in 2012, the community has shown a consistent energy and enthusiasm for this important topic, really driving it throughout communities and networks.

At this year's World Economic Forum Annual Meeting, the community came together in a private session to discuss the current results and future plans for the initiative. With many participants from various industries and the public sector, the Meeting in Davos determined next steps and objectives for 2013.

The topic gained a lot of interest, not only in official sessions, but even in the hallways, as noted by FT.com's Gillian Tett.

This newsletter is dedicated to the discussions held at the PCR sessions at the Annual Meeting. In addition, it highlights the support from the UK Government, as William Hague, Secretary of State for Foreign and Commonwealth Affairs of the United Kingdom, signed the Principles at the Meeting. The UK has joined a great group of leaders from the public and private sectors.

Read more about this topic on the BBC news website at: http://bbc.in/XAZO5a

Over 80 companies and government bodies across 18 sectors and 26 countries have now joined the PCR initiative.

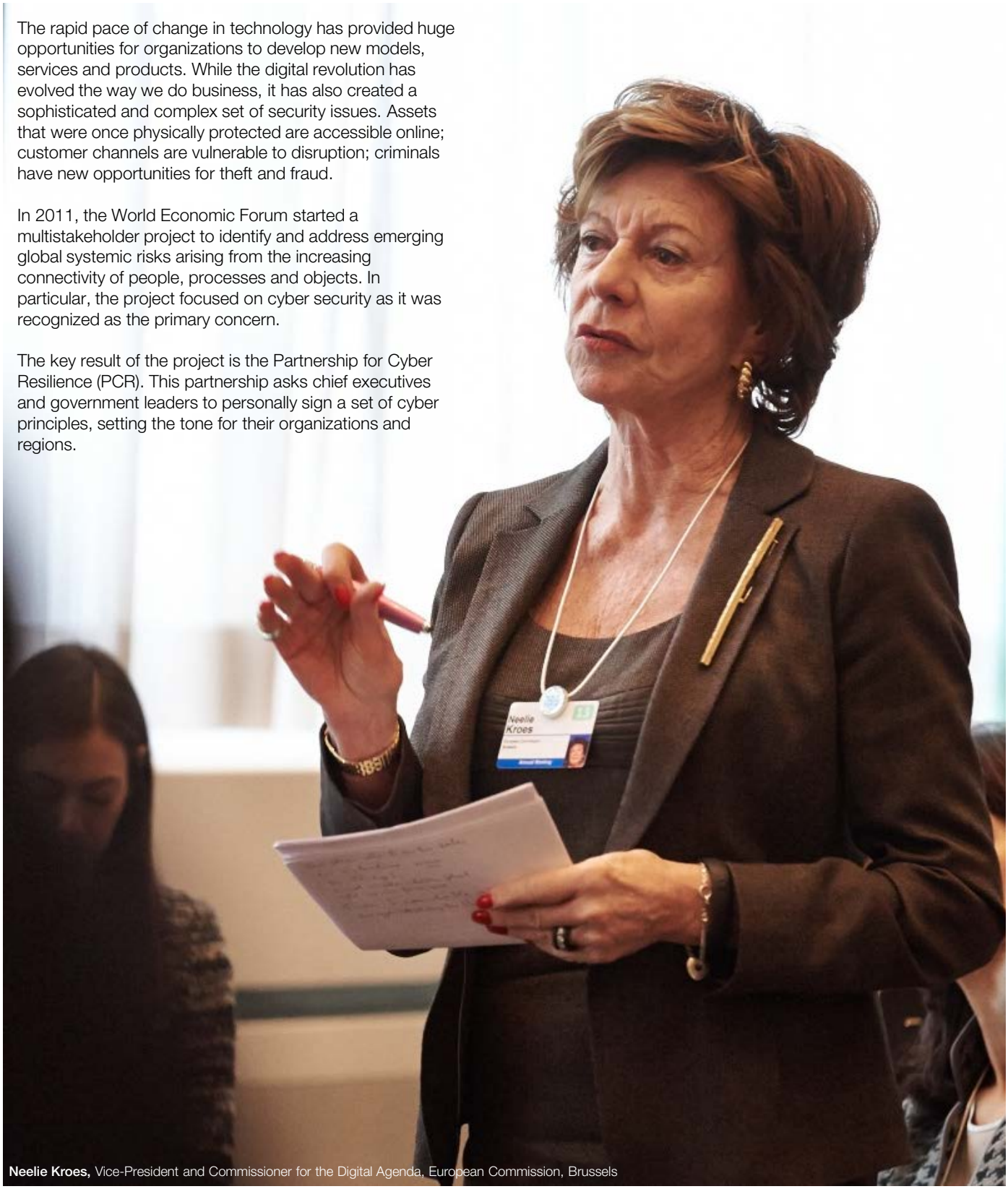
The consistent effort from the PCR community is what drives societal change. Thanks to the PCR Partners, this community is building global cyber resilience, moving the needle on cyber risk in this hyperconnected world.

Risk and Responsibility in a Hyperconnected World – Partnering for Cyber Resilience Private Session Summary

The rapid pace of change in technology has provided huge opportunities for organizations to develop new models, services and products. While the digital revolution has evolved the way we do business, it has also created a sophisticated and complex set of security issues. Assets that were once physically protected are accessible online; customer channels are vulnerable to disruption; criminals have new opportunities for theft and fraud.

In 2011, the World Economic Forum started a multistakeholder project to identify and address emerging global systemic risks arising from the increasing connectivity of people, processes and objects. In particular, the project focused on cyber security as it was recognized as the primary concern.

The key result of the project is the Partnership for Cyber Resilience (PCR). This partnership asks chief executives and government leaders to personally sign a set of cyber principles, setting the tone for their organizations and regions.



Neelie Kroes, Vice-President and Commissioner for the Digital Agenda, European Commission, Brussels

Dina Deliwe Pule, Minister of Communications of South Africa

At the World Economic Forum Annual Meeting 2013 in Davos, Switzerland, chief executives, ministers and heads of state met in a highly interactive private session that sought to address the challenges for the second year of this initiative.

Jolyon Barker, Deloitte's Managing Director for the TMT Industry serves as the key adviser for the Forum on this topic and facilitated the session in Davos, together with BBC World Anchor Nik Gowing. Neelie Kroes, Vice-President and Commissioner for the Digital Agenda at the European Commission shared the European perspective with the group.

Jolyon Barker, Managing Director, Global Technology, Media and Telecommunications, Deloitte Touche Tohmatsu Limited, United Kingdom

Carlos López Blanco, Director, Public Affairs, Telefonica, Spain

Lynn St Amour, President and Chief Executive Officer, The Internet Society (ISOC), Switzerland

Participants convened in several breakout groups, each focusing on a particular interest area: financial services, led by Phil Harrington (CA); critical infrastructure, led by Ray Johnson (Lockheed Martin); ICT, led by JP Rangaswami (Salesforce.com); national coordination, led by Francis Maude (Cabinet Minster, UK Government); Swiss public-private collaboration, led by Andre Kudelski (Kudelski); and regional coordination, led by Robert Wainwright (Europol).

Participants discussed the following questions:

1) What is the single biggest cyber-related risk in your area?
2) Are the proposals from your experts good next steps for action?
3) What should be the focus of collaborative actions in 2013?

Concerns about cyber security are increasing rapidly in line with the number of attacks. Participants focused on how companies, governments and regional organizations can address the threat without stifling the Internet's potential as a driver of innovation.

The conversation covered how companies can best keep cyber issues on the corporate radar screen, inform shareholders and others about their efforts in tackling them, and help companies in developing countries address cyber threats.

Ellen Richey, Chief Enterprise Risk Officer, Visa, USA.

George Kvirikashvili,
Minister of Economy and Sustainable Development of Georgia

As cyber security comes to the fore, the biggest risk companies face is losing the trust of their stakeholders. While the dangers loom increasingly large, too few companies understand the specifics of the threats they face or what to do about them. These dangers relate not just to doing business today, but to the smooth operation of products and services already out there – from power plants and large buildings, to transport networks and energy exploration.

Participants agreed that the greatest vulnerability relates to mobile devices that now contain not just a wide range of personal and corporate data, but can perform a variety of functions – from unlocking doors to running systems. This means that as cyber attacks become more sophisticated, the surface area of exposure expands.

Murat Sonmez, Executive Vice-President, Global Field Operations, TIBCO Software, USA

While cyber threats present the single biggest threat faced by most large corporations, the clock cannot be turned back. Companies have no choice but to fight back and win.

It was broadly agreed that cyber security should be a regular item on the agenda of board meetings. Equally important is hard wiring these issues into management practice throughout the organization. It needs to become a natural reflex, “like brushing your teeth”.

This is not yet the case. In Europe, only 26% of companies have a cyber security strategy. To turn the corner, they must move beyond awareness to action by including cyber security as an accepted part of the cost structure. Neelie Kroes, Vice-President and Commissioner for the Digital Agenda, European Commission, Brussels, urged participants to engage with her office to provide input on the upcoming EU Cyber Strategy, due to be released shortly after Davos.

Finding ways of sharing information about cyber security with stakeholders is crucial. It has direct implications for performance and valuation, and will increasingly be demanded by analysts and others. Including this as a standard item in annual reports is one way of doing so, but there is a danger of reducing a central business concern to a few sanitized lines in the annual report.

Marco Comastri, President and General Manager, Europe, Middle East and Africa, CA Technologies, Switzerland

While participants saw transparency as important, some speakers questioned whether total openness is appropriate because of its potentially negative implications for a company's business and its reputation. Further, before getting too prescriptive about how to report, it is important to clarify what exactly they should report on. One suggestion was that companies might begin by divulging attempted breaches rather than all breaches.

The key discussion topics during the private session included the following:

1. Develop the cyber agenda for board meetings, incorporating key questions for boards to ask on their organization's cyber resilience.
2. Develop ways to increase cyber transparency, by executing a study on current cyber resilience reporting and transparency in annual (financial or CSR) reports.
3. Research existing national cyber strategies to analyse maturity levels, strengths, weaknesses, commonalities and differences.
4. Explore the possibility of a Cyber Resilience Development Foundation, a fund to help developing nations improve their capabilities, supported by mature organizations and nations in the form of cyber CSR.

Larissa Herda, Chairman, Chief Executive Officer and President, tw telecom, USA

Building Cyber Resilience – Public Panel Discussion

There may be an active arms race with the bad guys, but the consensus of the panel in this session, Building Cyber Resilience, is that the good guys are at least battling to a draw most of the time, but only so far.

At this year's Annual Meeting, the Partnering for Cyber Resilience initiative formed part of the public programme as well. During an interactive session, panelists focused on the question: How can countries and companies develop cyber resilience in a hyperconnected world?

Now that cyber security has become a mainstream topic, the challenge is not to convince stakeholders they need to be concerned and to take more precautions. The conversation is at a new level. The dialogue calls for greater transparency by businesses that have been attacked and hacked to acknowledge what happened to them so that others can learn.

Boards should understand that cyber risks are among the top three risk issues they face now, and they should be examining corporate preparedness annually. Finally, governments must share responsibility for enforcement and provide better oversight.

Ian Livingston, Chief Executive Officer, BT Group, United Kingdom.

Some experts in the field now distinguish among at least three main forms of cyber attackers – those by cyber criminals, those that are state-sponsored and those by cyber terrorists. Given this categorization of three types of attackers, one panellist advised that lumping them together as the same risk would be like saying that seeking medical care, hiring body guards and getting a massage are the same.

After all, they are all about taking care of your body. However, they are not the same at all and each calls for a different strategy. The same philosophy applies to combating cyber security threats.

Finally, the suggestion was made that we should look to cloud computing not as a source of increased cyber risk, but for answers to help build better practices and protections against cyber attacks.

As commented by rapporteur **Paul Sagan**, Executive Vice-Chairman, Akamai Technologies, "a global cyber defence shield is one of the best ways to aggregate data about risks and attacks, and to mount a potent defence against hackers. Rather they are continuing to only try to lock down every device and build a bigger wall around your cyber assets, look to start your first line of defence out in the cloud, closer to where the bad guys live. You no longer just have to play defence where your data and applications reside."

Panel speakers for this discussion included: **Francis Maude**, Minister for the Cabinet Office of the United Kingdom; **Gary Regenstreif** Editor, Special Projects, Reuters, Thomson Reuters, USA; **Eugene Kaspersky**, Chairman and Chief Executive Officer, Kaspersky Lab, Russian Federation; **Neelie Kroes**, Vice-President and Commissioner for the Digital Agenda, European Commission, Brussels; and **Ian Livingston**, Chief Executive Officer, BT Group, United Kingdom.

Paul Sagan served as Rapporteur for this session. Read his insights from the session at: http://www.weforum.org/sessions/summary/building-cyber-resilience

United Kingdom Joins the PCR Initiative

Trust in the digital realm is essential for innovation and growth in all industries and sectors and no one organization can resolve cyber security alone. That is why UK Foreign Secretary Hague joined the more than 80 global leaders across public and private sectors that are committed to working together on cyber resilience.

The community welcomes British Foreign Secretary William Hague's signing of the World Economic Forum's Partnering for Cyber Resilience principles, which complements the UK's 10 Steps to Cyber Security for Business Executives. This guidance for industry on meeting cyber security challenges is an excellent example of putting the Principles in practice. The 10 Steps to Cyber Security booklet was launched last September and sent to chief executives of a number of the UK's largest companies.

On signing the cyber resilience Principles, the Foreign Secretary said: "We hope that signing the Principles on cyber resilience will encourage business leaders all over the world to lead the way in creating shared principles for a resilient and thriving internet. The Internet has a critical role to play as an engine and facilitator of economic growth. Cyberspace must be secure and reliable so that it is trusted as a medium for doing business but at the same time free and open to evolve and innovate naturally. Governments should support the key role of the private sector in creating a trusted and open place to do business both at home and abroad.

The Principles will help us all – individuals, companies and governments – in our shared aim to promote a safe and secure digital environment to do business."

In addition to company guidelines, the UK announced a new Global Cyber Security Capacity Building Centre last October. The centre will be hosted within the UK's network of Centres of Excellence for Cyber Security. Currently, eight universities have been awarded this status based on their world-class research capability in this field.

Francis Maude, The UK's Minister for Cyber Security at the Cabinet Office, is participated in a number of events at the Annual Meeting in Davos aimed at bringing industry and governments together to tackle the global issue of cyber resilience and security.

Speaking in Davos, the Minister said: "Cyber security is a shared, global challenge – our companies operate in a global marketplace. The cyber threat knows no geographical boundaries and it matters that those we connect to are secure as well. In the UK we have put in place a transformative National Cyber Security Programme which hinges on a real and meaningful partnership with industry. We are very proud to be members in this global initiative. We hope that our guidance for businesses and the Global Capacity Building Centre, which form part of our increasing efforts to make cyberspace a secure and stable environment in which businesses can grow."

Over the coming months, this initiative will build on the insights generated at Davos and the sessions held in 2012 and the community will work with the World Economic Forum in subsequent events to grow the Principles for Cyber Resilience partnership and work on the agreed upon actions.

"We hope that signing the Principles on cyber resilience will encourage business leaders all over the world to lead the way in creating shared principles for a resilient and thriving Internet."

Francis Maude, Minister for the Cabinet Office, United Kingdom, speaking at a press conference on joining the Partnering for Cyber Resilience initiative.

Cyber Security. Evolved made its debut during the Annual Meeting 2013, a follow-up to last year's *Companies Like Yours* cyber video. Click the image above to view the video.

JP Rangaswami, Chief Scientist, Salesforce.com, United Kingdom

Ray Johnson, Senior Vice-President and Chief Technology Officer, Lockheed Martin Corporation, USA

Rosemary Leith, Director, World Wide Web Foundation , United Kingdom

Rob Wainwright, Director, Europol (European Police) , The Netherlands

The 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

Contact:

Elena Kvochko
Tel.: +1 646 462 8750
E-mail: elena.kvochko@weforum.org

weforum.org/cyber

cyberresilience@weforum.org

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.

We are also grateful for the commitment and support of Deloitte in their capacity as project adviser.

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

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.