Partnering for Cyber Resilience

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

January 2013 Newsletter

In this newsletter:

World Economic Forum Annual Meeting 2013, Davos-Klosters, Switzerland

The Annual Meeting 2013 will convene this year under the theme "Resilient Dynamism". This reflects the need for business leaders to adopt a "risk-on" mindset that allows their organizations to perform with strategic agility while at the same time retaining strong resilience in the face of global challenges.

In line with this overall theme, the Partnership for Cyber Resilience initiative will once again convene global leaders to improve systemic cyber risk management. Launched at Davos in 2012, a multi-industry and public-private community of companies and governments supported a common set of principles to guide leaders in their duty to ensure the resilience of their organizations. The commitment shown to these principles has driven action at the individual organization level and has enabled a broad-ranging dialogue covering multiple business and policy concerns. The community now has the opportunity to move from coordinated individual action to shared action.

At this year's Annual Meeting, the community will focus on the following:

1) What should be the key priorities for this multistakeholder group in catalysing awareness, understanding and action on cybersecurity?
2) What are the key actionable insights for leaders across all domains for 2013?
3) What innovations for collaboration between the private and public sectors are emerging and working best?

Participants will convene in breakout groups to discuss cyber issues for existing or emerging clusters of activity and innovation, such as specific industry groups, regions or nations. Participants will be asked what success means in the context of cyber resilience, which actions they should take for 2013, and what they can collectively do to develop systemic solutions. Results will be summarized in the next edition of this newsletter.

The Partnering for Cyber Resilience Conference 2012 Dublin, Ireland and Washington DC, USA

Gaining commitment and building awareness

Digital transformation makes the protection and resilience of our shared infrastructure a strategic concern for our economic and social well-being. The ability to provide a trusted environment for individuals and businesses to interact online is a critical enabler for innovation and growth.

In recognition of this, and in response to the growing threats and risks in a digitally interconnected world, over 80 companies and government bodies across 15 sectors and 25 countries have joined forces to create the Partnering for Cyber Resilience initiative. Together, the leaders of these organizations have signed a set of Principles, which demonstrate their commitment to play their role in providing a resilient digital environment.

This initiative is at the forefront of changing the conversation around resilience to cyber risks – from being a narrow technical specialization to being a topic of core strategic concern for chief executives and government leaders worldwide.

On 5 December and 12 December 2012, the World Economic Forum organized two sessions with the participants of the Partnership for Cyber Resilience initiative. The sessions were held in Dublin, Ireland, and Washington DC, USA. Among the key questions raised:

1) What are the challenges and lessons learned in dealing with cyber risks?
2) How do we collaborate and work together between the public sector and the private sector?
3) What should be the focus for the year 2013?

The Dublin Discussions

Domestic and international cyber frameworks

There is widespread recognition that the current legal framework, and associated institutional capabilities, are not equipped to deal with many cyber security and cyber criminal issues, both at the national and international level.

Improving dialogue

There are many overlaps in the work of various international institutions working on cyber security, but at the same time there is a lack of awareness of the work that is being done internationally. It is necessary to structure international dialogue to avoid duplication of efforts.

Tools and solutions

Broadening and deepening the tools for public and private sector executives will help make the leaders and organizations more resilient. Assisting developing countries was recognized as an important way to ensure more secure cyber environments globally. Industry, region or issue specific case studies on cyber security ensure relevance to the intended audience(s).

Leverage the power of leaders

There remains a continued need to engage leadership communities within and outside the Forum to raise levels of awareness and understanding around cyber resilience.

The partnerships signatory base represents a large network with significant media/social media reach that can be activated to educate global audience and the public.

The Washington DC Discussions

Changing the dialogue across sectors and countries

Many participants noted that governments lack robust ways of identifying, analysing and communicating cyber risks. From the industry perspective, improved information sharing is critical. However, the appropriate legal environment needs to be established to allow better collaboration.

Tools for decision-makers

Case studies, which could be written in partnership with top business schools, companies and organizations, can become additional useful tools. There has yet to be a framework developed that would be applicable across different countries.

Reporting and information

Some participants suggested that companies should report on their cyber security efforts in their annual reports. There are a number of alternative models behind this suggestion, e.g. the reporting could be voluntary or mandatory; it could be about breaches, capabilities or responsibilities; it could be captured within the enterprise risk section or the CSR section.

There was a general consensus that a voluntary approach that covered capabilities/ responsibilities and was based on social norms/peer pressure (like CSR or environmental issues) would be more effective than mandatory reporting of breaches, which would lead to box ticking and miss the opportunity.

Direction for 2013

Clear themes emerged in the discussions throughout the year and the concluding sessions with the key stakeholders in Dublin and Washington DC.

The overarching theme was the need to change the conversation – away from cyber security as a cost, as an add-on or afterthought, and as an issue to be delegated, towards a perspective on cyber resilience as a core strategic issue for the boardroom and top policy-maker. In particular, there is a need to link the issue to the opportunities that ICT connectivity is providing.

In particular, the key message that many feel has often been missed, but is now becoming increasingly clear, is that cyber resilience is a critical economic enabler – for both companies and countries.

Furthermore, among those that are aware and committed, excellent collaboration and innovation can be seen across many countries and industries around the world. However, this is just the start, and further dialogue and coordination is required to promote collaboration between sectors and geographies. These dialogues will be the path to advance the dialogue and highlight successes around shared issues such as information sharing, cross-industry issues and cross-border question.

The twin challenges that the initiative aims to tackle are to:

1) Continue to promote leadership awareness and understanding
2) Provide a platform to connect networks to tackle shared issues

A number of tools were proposed to support these overarching objectives, such as industry and issue-specific case studies, improved index data on country cyber resilience, and continued development in the breadth and depth of existing tools like the maturity curve and shared definitions. The list was substantial, but leveraging the resources of the network, it may be possible to make progress on a modest number of these in 2013.

Annual Meeting 2013

The World Economic Forum Annual Meeting in Davos is an opportunity to get executive support for this approach in 2013 and to get additional perspectives for consideration.

However, it is also an opportunity to gain executive leadership commitment for action. Specifically, two suggestions emerged as being relevant for the Davos audience:

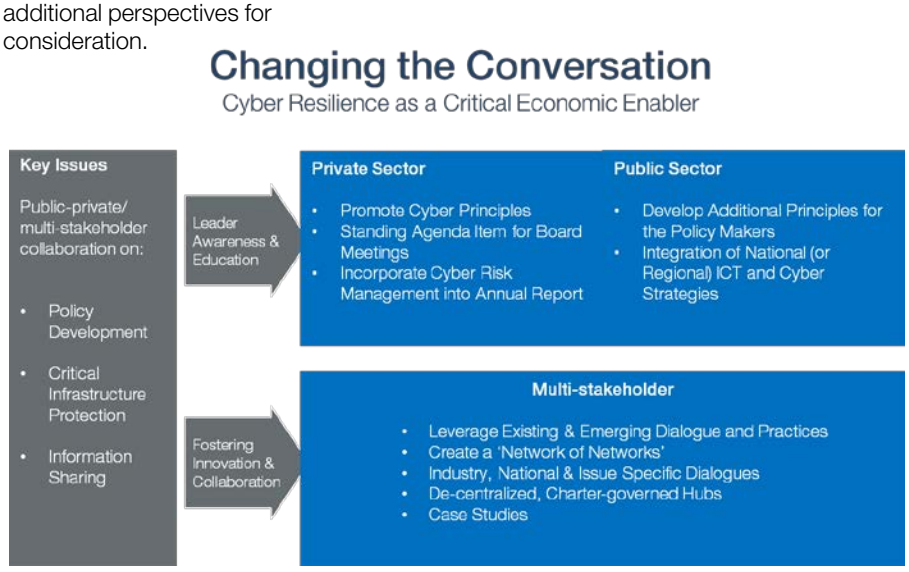
1) Commit to have cyber resilience as a standing item on the board agenda (specific details, such as frequency and governance mechanism, to be determined by the company themselves)
2) Commit to include a statement or section on what the company is doing to fulfil its responsibility to a resilience shared digital environment within the CSR section (or other) of its Annual Report (applicable to reports published after 1 July 2013)

Additional Proposal

In addition to these two suggestions, a third proposal was made by the participants:

3) Create an independent fund from CSR contributions to support capacity building for developing and emerging economies (e.g. helping develop CERTS in Africa)

Further discussions on this final proposal are required, however early testing of the idea has met with a very positive response. Feedback would be most welcome.



New Signatories to the Partnership

The World Economic Forum would like to extend a warm welcome to the new members of the partnership:

- AcceptEmail
- Argent Consulting
- BAE Systems
- Barclays
- Basic Element
- The Boston Consulting Group (BCG)
- Cassidian
- Clifford Chance
- Deutsche Bank
- EMC
- FIS
- Government of Paraguay
- HCL
- Hewlett Packard
- Huawei
- Infosys
- Internet Security Forum (ISF)
- IS Group
- Mahindra Group
- McKinsey & Company
- RR Donnelley
- Olayan Group
- Oman CERT
- Port of Rotterdam
- SABIC
- SAP
- Schiphol Group
- Schuberg Philis
- Transparent
- Unilever
- Vimpelcom
- Wipro

Open Call for Forum:Blog

The World Economic Forum's ICT Team is encouraging submissions from partners for Forum:Blog.org on cyber security and more general IT industry developments. The suggested length is 700 words, but submissions of any length will be considered.

Proposed topics and posts may be sent to Elena Kvochko, elena.kvochko@weforum.org

"We're seeing an increase in sophisticated attacks that are specifically targeted on a particular organization, sector or country."

Martin Sutherland, Managing Director, BAE Systems Detica

About BAE Systems Detica

BAE Systems Detica delivers information intelligence solutions to government and commercial customers. The company helps them collect, exploit and manage data so they can deliver critical business services more effectively and economically. BAE Systems Detica also develop solutions to strengthen national security and resilience. Detica is part of BAE Systems, a global defence and security company with over 93,000 employees worldwide.

Q&A with Martin Sutherland, Managing Director of BAE Systems Detica

Why do you support Partnering for Cyber Resilience?

We live in a hyperconnected world and cyber crime is a very real threat to global economic prosperity and security. Cyber attacks are growing in number and becoming ever more varied as attackers refine the methods they use; so a forum that brings together commercial organizations to explore how we can work together to raise standards and deal with the issue has to be a good thing.

Companies like BAE Systems Detica all have a role to play in contributing to an open, secure and resilient online space. No single organization can overcome the problem; it has to be a concerted effort across the private and public sector. Determining a set of principals and setting a policy and framework for cyber security is key and that is why we are very keen to support the World Economic Forum's Partnering for Cyber Resilience initiative.

What do you see as the main strength of the Partnership?

The World Economic Forum brings together business leaders at the highest level and it is exactly the right place to raise awareness of the issue of cyber security, the growing threats we face and the need to actively promote and develop cyber resilience. In 2012, we have seen a ten-fold increase in cyber attacks, which now come from more groups of attackers than ever before and from an increasing number of countries.

The Forum brings the issue to the global stage and I believe that Partnering for Cyber Resilience will raise awareness among chief executives and at board level – as well as at government level – of the need for greater vigilance and the need to put cyber security at the heart of their organizations.

What is your main concern regarding cyber resilience?

Our concern at BAE Systems Detica is the sheer scale of cyber threats and successful attacks. We face a multitude of attackers from single hacktivists operating from their bedrooms to industrial organizations, supported by foreign states to foreign states operating in their own right.

Clearly state-sponsored adversaries have far greater resources at their disposal than the lone hacktivist and their motivations are more sinister. They also have the potential for far greater impact on global social and economic well-being.

We are seeing an increase in the incidence of sophisticated attacks that are far more focused and are specifically targeted on a particular organization, sector or country. We are also seeing commercial organizations experiencing the types of attacks that previously were only used against government and militaries. We have seen examples of cyber attacks that had the potential to cause serious physical and environmental issues, including recently the Shamoon attack on Saudi Aramco, the worlds largest oil producer.

This was a vivid demonstration of the ease at which large organizations, which control oil refineries, petrol stations and large parts of national infrastructure, can be targeted. We in the cyber security industry know this the tip of the iceberg, and many attacks are unreported or worse undetected.

"TMT organizations now recognize that information security is fundamental to their business, and not just a compliance issue anymore."

- **Jolyon Barker, Managing Director of the Global Technology, Media and Telecommunications (TMT) Industry Group, Deloitte Touche Tohmatsu**

About Deloitte

The Deloitte TMT industry group consists of more than 10,000 TMT member firm partners and professionals in 45 countries. Jolyon Barker is the knowledge partner for the World Economic Forum's Risk and Responsibility in a Hyperconnected World project and the Partnering for Cyber Resilience Initiative.

Key Findings from Deloitte's 2013 TMT Global Security Study

Deloitte recently published their annual worldwide study into information security practices in the Technology, Media and Telecommunications (TMT) industries. Jolyon Barker, Managing Director, Global Technology Media and Telecommunications at Deloitte and project adviser to the World Economic Forum, summarizes the results.

One of the key findings this year is that security is increasingly seen as a value driver for businesses. The main question for TMT organizations today is how to achieve information security. According to this year's study results, the top security initiative for 2013 is to create a strategy and roadmap for information security. The results of the study indicate that organizations are now focusing on information security because their customers and the marketplace demand it, not just because regulations require it.

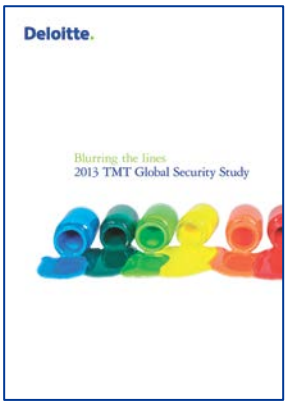
The study also points to the relevance of the human element; 70% of respondents rate their employees' lack of security awareness as an "average" or "high" vulnerability. The report also links this finding to two recent trends – "Bring Your Own Device" and "Rogue IT" – where employees use (cloud-based) software outside of the organization's reach.

Lastly, organizations see third party risk and vulnerability as their biggest threat. This is a growing concern, developing from one of many to the main worry for organizations in just a few years. This reliance on third parties and the subsequent risk speaks to the hyperconnected world, in which no organization is really independent.

Jolyon Barker adds: "The big question is what to do next. TMT organizations face an onslaught of new and growing security threats. All of these trends are converging to create an environment where traditional security boundaries are blurry or even non-existent. How can a TMT organization build a strong way of defence against cyber attacks in a world without boundaries?"

At the same time, TMT organizations are trying to figure out how to manage new technologies such as mobile and cloud computing — technologies that promise to dramatically improve how businesses operate, but which also present significant new security challenges and risks.

The report offers further detail on findings and some suggested responses. Read the full report here: Download report



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:

Derek O'Halloran
Head of IT Industry
Tel.: +1 646 371 3757
E-mail: doh@weforum.org

Elena Kvochko
Project Manager
Tel.: +16464628750
E-mail: elena.kvochko@weforum.org

Alex de Leeuw
Project Manager
Tel.: +1 347 882 5811
E-mail: adl@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