

Partnering for Cyber Resilience

September 2012 Newsletter

Public Sector Support for Partnering for Cyber Resilience Initiative

In this newsletter:

New signatories

Annual Meeting of New
Champions

The PCR Conference

From PCR Members:

- Kaspersky
- Sonae

The Grand Conference

Calendar

Metrics

Resources

New Signatories to the Partnership

Since the last edition of this newsletter, the Organization of American States (OAS), Desjardins, Sonae and the Ministry of Information Technology and Communications of Colombia have joined the Partnership for Cyber Resilience (PCR). The support from OAS Secretary-General José Miguel Insulza and Diego Molano Vega, Colombia's Minister for Information Technology and Communications, is indicative of the increasing support of the public sector for the Partnership.

The OAS Secretary-General, Jose Miguel Insulza, stated that "joining the World Economic Forum's Partnering for Cyber Resilience is another demonstration of our organization's commitment to promoting cyber security, not just in the region but worldwide.". He called on other governments and organizations to join this important initiative. Secretary-General Insulza added that, "recognizing the value that new technologies have for development and security, the OAS is making great efforts to contribute to their promotion and to stimulate public-private interaction in issues as delicate and relevant as cyber security."

With the addition of Sonae and Desjardins, the total number of Partnership members has risen to 47. The members are based in 18 different countries, from all major regions, and represent 15 different sectors. Most members come from the Information Technology, Banking and Capital Markets, and Telecommunications sectors.



José Miguel Insulza, Secretary-General, Organization of American States (OAS), during the World Economic Forum on Latin America in Rio de Janeiro, Brazil, on 28 April 2011.

Annual Meeting of the New Champions – PCR Private Session Summary

During the Annual Meeting of the New Champions 2012 in Tianjin, People's Republic of China, on 11-13 September, the Partnering for Cyber Resilience initiative held a private session to discuss the following questions:

1. What is the balance between policy, regulation, self-governance and bottom-up governance?
2. Can common principles align policy-making across multiple jurisdictions?
3. What are the basic legal and enforcement capabilities of a responsible actor in the global economy?

Notably, participants considered that creating security standards that reach beyond national borders must be led by business. The private sector has the knowledge and the self-interest to create strong security principles. It is familiar with the risks, failures and consequences of policies that are inconsistent across countries.

One participant noted that, realistically, only so much security is achievable. Improving will be a collective effort involving a new awareness of risks and security measures to protect digital assets.

The key summary points :

1. Public sector participants recognized the complex and global nature of the issue and their own constraints. They emphasized the need for the private sector to take a leading role.
2. Government representatives shared innovations aimed at enabling the private sector.
3. The need to share successes and best practices in private-public innovations was highlighted.
4. Governments also discussed the challenges of aligning activities across agencies and departments.

“The foremost challenge is to educate policy-makers. The second is to define the institutional framework to deal with the issue.”

Participant at the Annual Meeting of New Champions 2012, Tianjin, People's Republic of China



“Our only way forward is modest - this is like treating a disease. We should practice wellness as our main goal.”

Participant at the Annual Meeting of New Champions 2012, Tianjin, People’s Republic of China

Annual Meeting of the New Champions – Creating a Resilient Cyber Economy

In addition to the private session, the Partnering for Cyber Resilience initiative supported an official programme session on Creating a Resilient Cyber Economy. The session focused on the question “How can the potential of the cyber economy be realized?”, by looking at the following dimensions:

1. Protecting digital privacy and reputation
2. Addressing international security threats
3. Building trusted data environments

The panelists included PCR signatories Tetsuo Yamakawa, Vice-Minister for Policy Coordination of Japan, Michael Fertik, Founder and Chief Executive Officer, Reputation.com, and Eugene Kaspersky, Chairman and Chief Executive Officer, Kaspersky Lab.

The full summary and video of the session can be found [here](#). Key outcomes of the panel discussion include:

- **Cyber warfare is real:** Either by hacktivists or nation-states; it is hard to be prepared. Business needs to better evaluate the risk of all of data being erased or exposed. It is important to understand the consequences of either of these happening.
- **Personal Data has value:** Systems will be created to help people capitalize on the value of their data and be compensated. Compensation comes in many forms, but as the value of personal data is better understood, systems will come along to capitalize on them in a way that is not subversive or necessarily nefarious.
- **Openness is the key to progress:** Regulation and a multistakeholder approach are requirements for progress, but the Internet has flourished under an open model with open standards and limited governance. It is likely that this is the best path on which to nurture and facilitate the cyber economy.



Partnering for Cyber Resilience Conferences

The World Economic Forum will send out invitations shortly to a set of multi-stakeholder events for the Partnering for Cyber Resilience community, to be held in **Dublin on 5 December** and in **Washington on 12 December**. Key public sector and business leaders will discuss the roles of the public and private sectors to build a resilient and trustworthy cyber environment.

The Conference will be held in two locations on two separate dates to gain a greater perspective and to accommodate broad participation.

Chief Executive Officers, public sector leaders, or the key advisers to the head of the Annual Meeting delegation in Davos will be invited to participate in these discussions, which will determine the agenda and direction of the cyber-related discussions at the Forum's Annual Meeting 2013 in Davos-Klosters, Switzerland, and the future of the initiative.

The agenda allows for extensive participant interaction, peer-group learning and network strengthening. In the morning, participants will join one of the two sessions, followed by a joint session in the afternoon.

Track 1 seeks to further develop and determine the future of the Partnership. Track 2 is intended for public sector representatives. It seeks to identify and share lessons learned and best practices for the public sector.

After these separate tracks, all participants will convene in a joint session for a keynote panel discussion and to enable public-private and international interaction and collaboration. The day ends with an informal networking reception.

Agenda

09.00 – 09.30	Welcome and Introduction
09.30 – 12.00	Track 1: PCR Signatories: Development and Future of the Partnership
	Track 2: Public Sector: Sharing Best Practices and Experiences
12.00 – 13.15	Lunch
13.15 – 14.15	Keynote Panel Discussion
14.15 – 17.00	Pathways to Global Cyber Resilience: Public-Private and International Cooperation
17.00 – 18.30	Networking reception

5 December 2012

Dublin, Ireland

Time:

09.00 – 18.30

Venue:

The Science Gallery at The Naughton Institute, Pearse Street Trinity College, Dublin 2
Dublin City, Ireland

12 December 2012

Washington DC, USA

Time:

09.00 – 18.30

Venue:

Organization of American States (OAS), General Secretariat Building
1889 F Street, N.W.
Washington DC, 20006, USA



Q&A with Eugene Kaspersky, Kaspersky Lab

Why did you support the Partnering for Cyber Resilience?

We enthusiastically signed up to the Partnering for Cyber Resilience since, as the name suggests, its aim is to increase resilience against the growing cyber threats that face us all together, as a partnership. And we are looking forward to sharing our expert knowledge and supporting the Partnership in its on-going development of guidelines, given the fast-changing cyber threat landscape.

Though fully cyber resilient businesses and economies are for now just distant future goals, the important thing is that something is being done now to reach those goals, as witnessed to by the Partnering's gaining increasing momentum. We all need to rise to the new challenges and overcome the constantly increasing and changing threats, especially when one considers that cyber attacks may soon come to represent the permanent conditions in which many organizations will have to work.

Completely new approaches will sometimes need to be applied in combatting the threats: in terms of hardware, this should involve a move toward secure operating systems and industrial control systems, while software would need to be re-written to be compatible therewith; that's quite a task!

Then there is the human element – often the weakest link in defenses, but normally the most straightforward to make resilient by basic education on cyber do's and don'ts.

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

I don't expect rapid change when it comes to international joint efforts where governments are involved – such initiatives always take time and that is natural. But at the same time, that is precisely why I am particularly keen to support the PCR, as its members are predominantly private-sector companies, and from a range of different industries. Besides, the PCR is a little bit different (to other cyber threat combatting projects), much like the World Economic Forum's Annual Meeting in Davos is different.

To me, the main differences are, first, in the audience – executive management, with the focus on top-down leadership for cyber risk management; and second, the understanding that combatting cyber threats needs to be resolved through a collaborative multistakeholder approach.

What is your main concern regarding cyber resilience?

Hactivism has done a lot to highlight the vulnerability of supposedly secure systems to penetration. At the same time, though purely cyber criminal break-ins (with no element of hactivism) are not as regularly reported in the press as hactivist attacks, this does not mean to say they are not taking place: it is hardly in the interests of either cyber crime victims or attackers to shout about attacks.



About Kaspersky Lab

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users. The company currently operates in almost 200 countries, providing protection for over 300 million users worldwide and more than 200,000 corporate clients globally.

In addition to that, since malware is forever increasing in sophistication, it can sometimes – particularly when deployed in state-backed weapons of cyber war – go unnoticed for months, even years, while continuing to do its damage, be that through cyber espionage or sabotage. Which brings me to the relatively new threat, not of cyber crime, but of state-backed cyber warfare, which is where I see the most potential danger to the world and life in it.

“...cyber attacks may soon come to represent the permanent conditions in which many organizations will have to work.”

Paulo Azevedo, CEO of Sonae, on joining the Partnering for Cyber Resilience Initiative

“Being connected is the new normal,” says Paulo Azevedo, Chief Executive Officer of Sonae.

Recognizing the interdependence of private and public sector organizations in the global hyperconnected environment, as well as Sonae’s role in contributing to cyber risk mitigation at the global level, Paulo Azevedo decided to join the Partnering for Cyber Resilience initiative in August.

“The way businesses and governments interact is drastically changing.”

Azevedo shared his insights on cyber resilience and why he, as a CEO, signed the Principles. “Hyperconnectivity and the evolution in cyber attacks require us to take ownership of cyber risk management.

The way businesses and governments interact is drastically changing and a renewed examination of roles and responsibilities is necessary. We can’t avoid dealing with the new risks and responsibilities that the hyperconnected world has brought us. This initiative offers a common set of principles, raising business standards and shifting mindsets from just securing perimeters to a focus on interdependence and resilience.”

Azevedo agrees that by committing to these principles, we can demonstrate leadership, accountability and best practice corporate governance in a digital world. This requires dedicated resources, staff awareness and leadership from the top.



About Sonae

Sonae is the largest retail company in Portugal with major partnerships in telecom, information technology, media and shopping centres. As of 2011, Sonae employed about 40,000 people, making it the largest private sector employer in Portugal. The company had a turnover of an estimated 5.72 billion Euro in 2011.

The Grand Conference, Amsterdam, 16 October

The Centre for Protection of the National Infrastructure (CPNI) will host a conference on 16 October in Amsterdam, the Netherlands.

CPNI took the initiative to organize a signing ceremony for the Partnering for Cyber Resilience initiative. Participants include European Commission Vice-President Neelie Kroes, UK Special Representative Baroness Pauline Neville-

Jones, and many C-suite executives and public sector leaders.

This conference aims to take cyber resilience from learning-by-doing to leading-by-doing. The event aims to develop leadership and create ownership to support sustained action.

Participants will meet other leaders in the field of cyber resilience in industrial control systems and smart grids.

The Grand Conference is an outreach of the EU-US Joint Working Group on Cyber Security and Cyber Crime organized by CPNI.NL and supported by the European Commission, European Network of Information Security Agency (ENISA), the US Department of Homeland Security (DHS), Alliander, TNO, the European Network for Cyber Security (ENCS), the Global Cyber Security Center (GCSEC) and Deloitte.

For more information, please visit www.thegrandconference.org



Calendar of Events 2012 - 2013



Following the Annual Meeting of the New Champions session in Tianjin, two key events are coming up for the Partnering for Cyber Resilience initiative.

On 16 October, CPNI will host a Grand Conference on the protection of national infrastructure. Secondly, the PCR conference on 5 December and 12 December will mark the first dedicated event for all PCR signatories.

Outcomes from this two-day conference will be discussed at the World Economic Forum Annual Meeting 2013 in Davos-Klosters, Switzerland.

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](#).

	September	October	November	December	January	February
Main Events	 <p>Annual Meeting of the New Champions, Tianjin, 11-13 Sept.</p>			<p>★ Partnering for Cyber Resilience Conferences ★</p> <p>Dublin, 5 Dec. Washington, 12 Dec.</p>	<p>Annual Meeting</p> <p>Davos, 23-27 Jan.</p>	
Other Events		 <p>CPNI conference on National Infrastructure, Amsterdam, 16 Oct. Organization of American States Virtual Cyber Briefing, 23 Oct.</p>	<p>ISF 23rd Annual World Congress, Chicago, 4-6 Nov.</p>	<p>SCADA and Process Control System Security Summit, Barcelona, 10-11 Dec.</p>		
Activities		 <p>Completion of interviews with public sector</p>		<p>Release of Deloitte TMT Security Study, 10 Dec.</p>		
Editorial Calendar	 <p>Newsletter 2, 24 Sept.</p>	<p>Newsletter 3, 29 Oct.</p>		<p>Newsletter 4, 17 Dec.</p>		

The Partners for Cyber Resilience

Aviation & Travel



Automotive



Banking & Capital Markets



Agriculture, Food & Beverage



Insurance & Asset Management



Information Technology



Media, Entertainment & Information



Multi-Industry



Private Investors



Professional Services



Government & Not-for-Profit



Retail & Consumer Goods



Supply Chain & Transport



Telecommunications

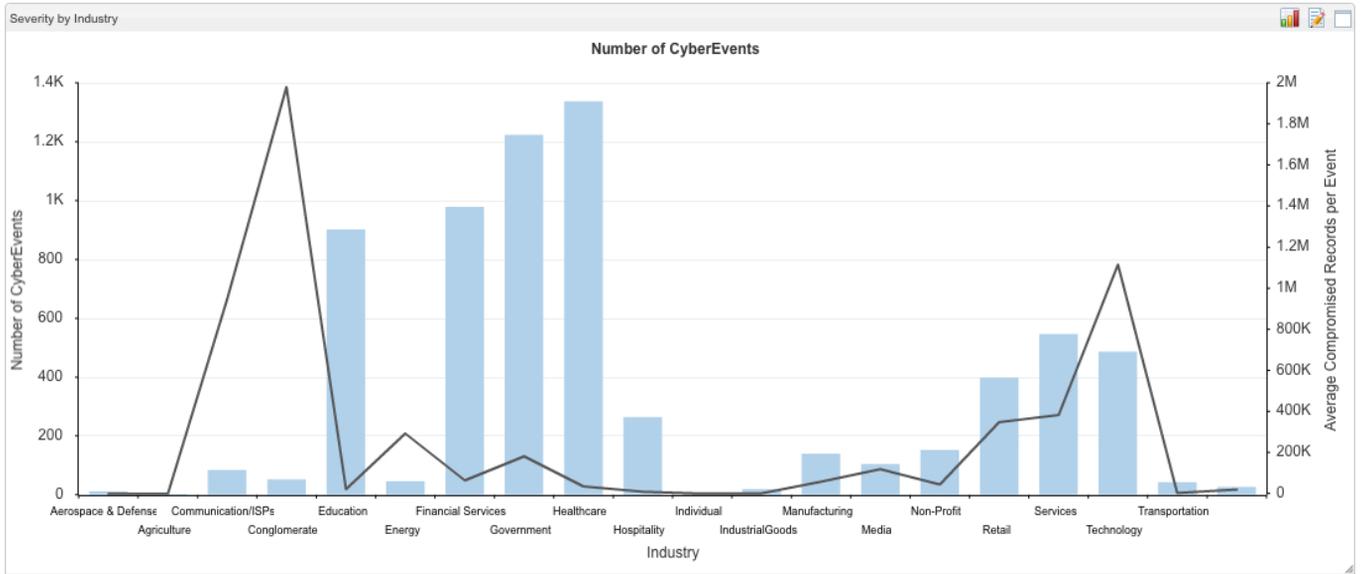


Energy Utilities & Technology



Is your logo incorrect or missing? Please [tell the team](#).

Key Figures: Cyber Incident Analysis



Data collected and analysed by CyberFactors. Left axis and bars show number of incidents per sector. Right

axis and line show average number of compromised records per event. Data has been accumulated since January 2005.

Key Figures: Partnership for Cyber Resilience Metrics

7 Fortune 500 Companies

7 Months since launch

18 Countries

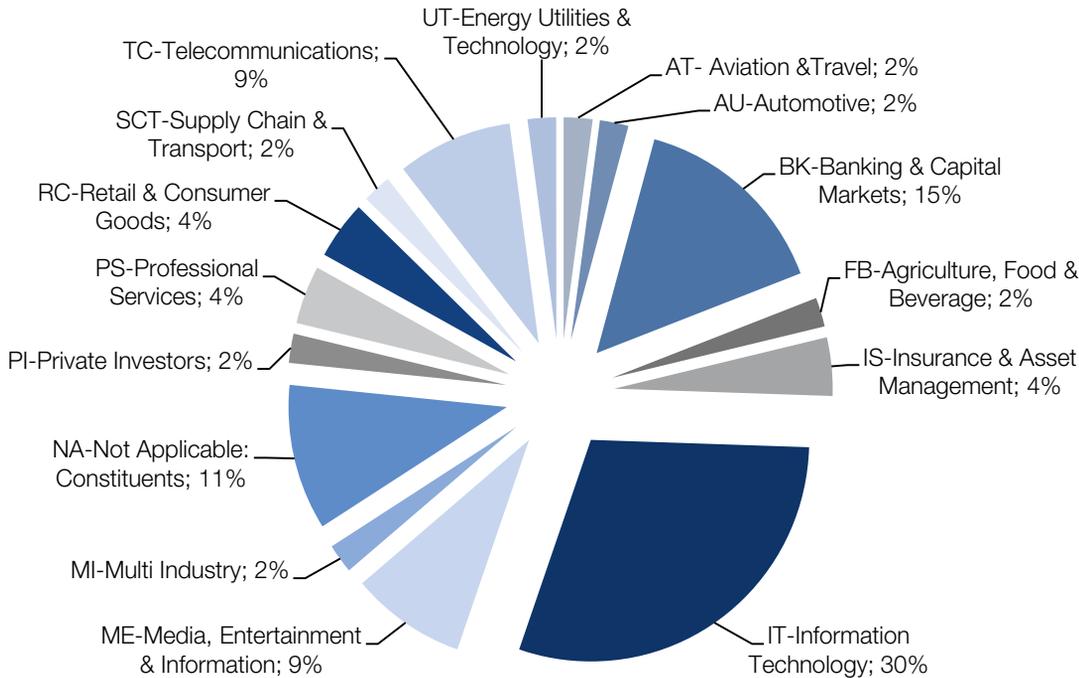
47 Business and Private sector leaders

15 sectors

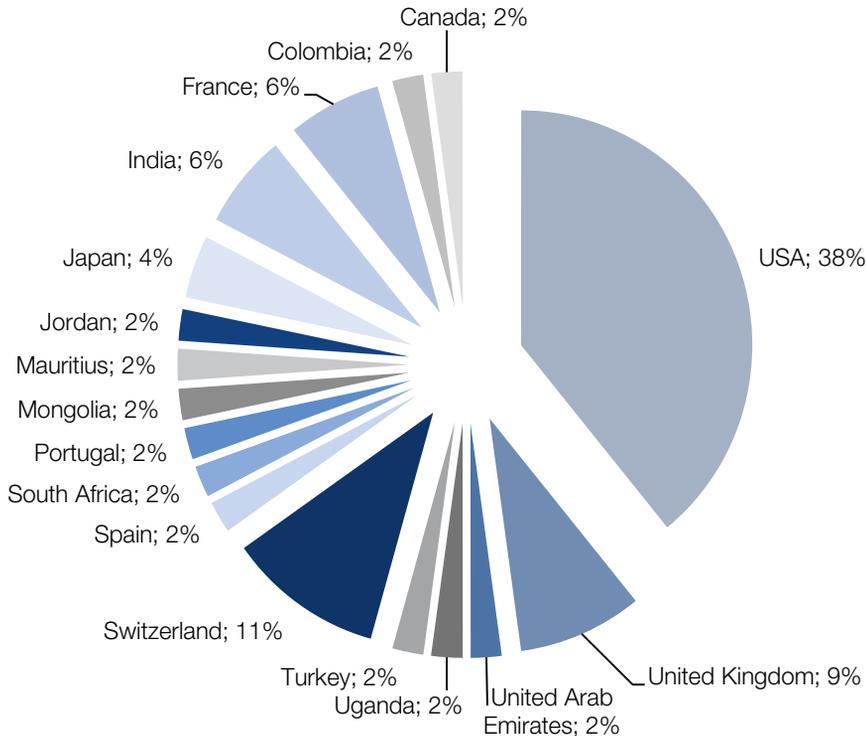
\$ 492,009,000,000
Total PCR Member Revenue (or if it were a country, the 20th largest economy in the world)

1,673,145
Total Member Employees

Key Figures: Cross-Industry Support



Key Figures: Gaining Global Reach



Contact:

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



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.