Cyber Scenarios Explored at the Annual Meeting of New Champions 2013

During the World Economic Forum Annual Meeting of New Champions 2013 in Dalian, People's Republic of China, senior business leaders and executives convened in a private session to explore current and future potential drivers and trends that will define the cyber ecosystem.

They also took a look at how each of the drivers would come together to form four potential scenarios by 2020:

Scenario A
Cyber threats increase, but sophistication of institutions does not. Businesses continue to reach the way they have in the past and the attack vendors continue to group together and increase in their relative sophistication.

Scenario B
Fears about cyber security slow down cooperation and trust. Sophisticated attack vectors are disseminated to a wider range of actors with some harbouring truly destructive intent. This ripples into implications for consumer purchasing habits, limiting business strategies and severely inhibiting government regulations

Scenario C
Technology and security become enablers to growth. Governments come together in the face of an ever increasing threat to facilitate the dramatic uplift in institutional capability and international cooperation.

Scenario D
After destructive attacks, public-private cooperation is improved, but consumer trust is eroded. A series of highly visible, destructive attacks shake the bedrock of consumer purchasing habits, forcing businesses to shift the way the act.

Participants discussed the implications of each of the scenarios. Some of the themes that emerged included:

- A push for new and innovative solutions from third-party vendors to help combat newer and more sophisticated threats
- A need to reformulate business strategy to consider changes ranging from countries in which companies feel comfortable operating in to the way they connected with consumers

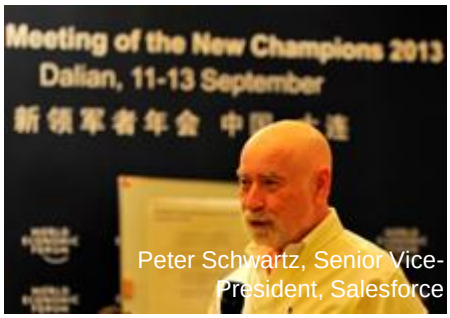
Cyber Scenarios Explored at the Annual Meeting of New Champions (cont.)

- A need for greater regional and international cooperation between nations to align regulations as well as prosecute criminals
- Opportunities will emerge for new businesses in insurance or risk markets to help businesses mitigate the potential downside from cyber risks

In the next phase of the initiative, the Partnership will working to further develop implications and define tangible recommendations.
A full summary of this and all other ICT sessions can be found in the *ICT Industry AMNC Report*


Christopher Mondini, Vice-President, Business Engagement, ICANN


Robert Greenhill, Managing Director, World Economic Forum, and Christophe Nicolas, Senior Vice-President, Kudelski Group



Peter Schwartz, Senior Vice-President, Salesforce

Taking Advice from Executives at Black Hat

As part of the broader Black Hat gathering of cyber security experts and researchers, 120 executives gathered for a full-day programme of leading-edge presentations and think tank discussions, including a roundtable led by the World Economic Forum's Partnering for Cyber Resilience initiative.

Key messages that experts felt should be surfaced to the top-level leadership network at the World Economic Forum included:

There is a need to educate top-level leaders about the infrastructure of the Internet, not just how reliant the world has become on connectivity for the normal functioning of society. At the macro level, this means highlighting and being very clear about the link between cyber capabilities and economic growth. This then needs to be supported by domain-specific pieces – executive one-pagers or training curricula for example – on particular industries or systems. What are the risks and challenges for the electrical power generation and supply, air traffic control, market exchanges, etc.?

More discussion needs to happen at all levels, including top leadership, about the trade-offs involved in expanding information sharing programmes. While there is still an incentive for organizations to share intelligence (commercial, liability, regulatory, equitable return from government), one key conceptual question is the optimal size of intelligence sharing networks in general. The trade-off is between coverage vs the scope for leaks of important information. For example, in the protection of critical infrastructure, governments need to balance bringing the private sector into the fold with "protecting the playbook".

The absence of a global enforcement mechanism was recognized. However, treaties and formal international organizations were seen as just one type of enforcement mechanism. In particular, experts felt that there is considerable scope and potential to use market mechanisms to encourage organizations to develop their capabilities in this space. The potential to develop mature risk transfer markets (insurance) is one clear example.

Gregory C. Case, Chief Executive Officer of Aon, on becoming resilient to digital risks

"Our advice is that companies should understand that cyber risk is no longer on the horizon. It is here, it is real ."

About Aon

Aon is the leading global provider of risk management services, insurance and reinsurance brokerage, and human resource consulting and outsourcing. Through its more than 65,000 colleagues worldwide, Aon delivers distinctive client value via innovative and effective risk management and workforce productivity solutions.

Q: How would you describe the level of concern about cyber risks among businesses?

Aon operates in 120 countries globally and it is absolutely clear that across the entire spectrum cyber is no longer an emerging risk; it has become a very important topic for management teams and boards of directors. Cyber risks are a reality in terms of what our clients see every day, whether it is mobile devices, cloud computing, social media or big data. Nevertheless, clients may still be underestimating the impact these risks might have. As businesses increasingly use technology to drive sales and efficiency, they also expose themselves to cyber risk vulnerabilities. Businesses are increasingly aware of the legal and reputational harms of cyber risks. We see that the costs of dealing with cyber risks go up year by year. Cyber threats can rapidly cut across regions and the world, and companies need to have a clear plan to understand, measure and mitigate cyber risks.

Q: How has the perception of cyber threats changed over time?

The perception and impact of cyber threats have evolved exponentially as organizations increasingly rely on new technologies and information assets. As the world is more connected than ever before, cyber risks must be addressed more quickly than many other types of risks. For example, the next wave of lawsuits against companies may be based on cyber risks. That is why quantification of cyber risks and benchmarking tools becomes very important. This will help you understand what kind of solutions you can get on the table: whether they are insurance-based solutions, risk-based solutions or operational solutions.

Q: What is the role of insurance-based risk mitigation solutions and what effect they might have on mitigating cyber threats?

Through our latest global risk management survey, we found that executives rank cyber risks very high, but are also underestimating the potential effects that cyber threats can have. We want to make sure that companies understand that cyber attacks are becoming more commonplace, but there are ways to understand them and calibrate them. Cyber risk is an enterprise risk management issue, an integrated type of risk which cuts across the entire firm. There are a number of evolving insurance-based solutions on the rise and we expect this to continue. We also expect an increased amount of capital to come into the industry to help mitigate cyber risks. But it is not just about insurance solutions. It is important to benchmark and implement operational improvements to prevent the risks before they happen in addition to trying to deal with the risks when they do happen, which is what the insurance-based solutions are targeted at. From our standpoint, it is important companies can identify, quantify and navigate the risks both operationally and from the insurance standpoint.

Q: What advice would you give to executives in terms of running their businesses in the evolving world of risks?

Companies should understand all aspects of cyber risk as best as they can: what it can do to your business, to its reputation and to your clients. How would you quantify and describe cyber risks in the context of your own business? What does it mean for your operating performance and balance sheet? Companies should increase their ability to predict what cyber risks can do to their business, where the risks are coming from and how they can control them to feel secure. The second piece of advice would be to create a game plan that you can adjust over time and that you can truly syndicate throughout the organization.

Building a Resilient Digital Society

The Grand Conference 2013, convening under the theme "*Building a Resilient Digital Society"*, will take place on 5 November 2013 in Amsterdam. The conference aims to make the critical infrastructure leadership aware of the importance of cyber resilience for their businesses and for society as a whole, especially as cyber resilience is a precondition for the digital transformation of our society. The conference's focus not only aligns with the Cyber Security Strategy of the European Commission, but also with the Forum's work on cyber resilience.

The target audience for the conference are mayors of leading Smart Cities in Europe, top government officials, and board members from critical infrastructure companies and their direct advisers and suppliers.

The main programme includes an international and European perspective on cyber resilience. Confirmed speakers are:

- Ivo Opstelten, Minister of Security and Justice of the Netherlands
- Tim Campbell, Author of *Beyond Smart Cities*
- Marc Canter, Chief Technology Officer, Digital City Mechanics
- Eugene Kaspersky, Chief Executive Officer, Kasperskylab
- Udo Helmbrecht, Executive Director, ENISA
- Dick Berlijn, Senior Board Advisor, Deloitte
- David Sandel, Founder, Gigabit City Summit

For more information, please visit www.thegrandconference.org.

DTCC White Paper Highlights Cyber Attacks and Global Systemic Risk

"Despite the positive results of risk mitigation efforts by the financial industry since the 2008 crisis, we urge continued vigilance and focus on systemic risks, especially given the growing interconnections and interdependencies in global markets."

- Noel Donohoe, Group Chief Risk Officer, DTCC

In its white paper *Beyond the Horizon: A White Paper to the Industry on Systemic Risk*, The Depository Trust & Clearing Corporation (DTCC) identified a number of emerging trends that could potentially impact the industry's ability to protect against new and unidentified threats to the financial system. The paper reports that despite progress over the past five years, systemic risks facing the global financial services industry are growing in complexity, are more difficult to anticipate and that new gaps continue to surface. Of these potential threats, one includes a rise in cyber attacks that can easily thwart US and EU industry safeguards and laws.

"Despite the positive results of risk mitigation efforts by the financial industry since the 2008 crisis, we urge continued vigilance and focus on systemic risks, especially given the growing interconnections and interdependencies in global markets," said Noel Donohoe, DTCC's Group Chief Risk Officer.

The white paper builds on DTCC's recent Systemic Risk Survey results and provides an overview of the key systemic risks facing the global securities industry as well as DTCC's role in systemic risk monitoring and mitigation. It highlights cyber security among a peer group of four other risks, including the impact of new regulations, counterparty risk, collateral risk and interconnectedness risk.

The issue of cyber security has emerged as a top systemic threat facing global financial markets and associated infrastructures, including the threat of Distributed Denial of Service attacks, attacks against systems containing transaction records, and risk of disclosure of restricted, confidential or Material Non-Public Information via compromise of internal systems. DTCC is calling for closer and more continuous engagement and action among all key industry participants on this issue to reduce the systemic risks facing global markets.

View the full paper at: http://www.dtcc.com/downloads/leadership/whitepapers/Beyond_the_Horizon_White_Paper_Systemic_Risk.pdf

View the video introduction at: http://www.dtcc.com/news/video/2013/beyond_the_horizon_systemic_risk.php

Calendar of Events 2013

- As part of this year's initiative, the Forum will be conducting an executive opinion survey and will be reaching out to the broader network to conduct an hour-long, one-on-one interviews to gain perspectives.
- Working group calls took place on in June, August and September 2013 across Europe, Asia and the Americas. To participate in these initiatives, and future sessions please contact elena.kvochko@weforum.org

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

*Planned

	October	November	December	January
Forum-led events	**Hyperconnectivity Day** New York City, USA 3 October			**Annual Meeting 2014** Davos, Switzerland 22-26 January
Project Dialogues			**Working group meeting** New York City, USA 12 December **Working group meeting** Geneva, Switzerland 5 December **Working group meeting** Tokyo, Japan 12 December	
Community -led events	**Healthcare Roundtable** Jersey City, USA 16 October **Banking Roundtable** New York City, USA 17 October **Cyberspace Summit** Seoul, Republic of Korea 17-18 October	**Grand Conference** Amsterdam, the Netherlands 5 November **OAS Regional Cyber Security Symposium** Montevideo, Uruguay 11-13 November		

Partnership 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

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 initiative, 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:

Derek O'Halloran
Head of IT Industry

Elena Kvochko
Manager
Information Technology Industry

cyberresilience@weforum.org