Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

04-May-2017

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Cancels & replaces the same document of 30 March 2017

Working Party on Security and Privacy in the Digital Economy

OECD EXPERT WORKSHOP ON IMPROVING THE MEASUREMENT OF DIGITAL SECURITY INCIDENTS AND RISK MANAGEMENT: TAKING STOCK OF PROGRESS AND PRIORITIES FOR INTERNATIONAL ACTIONS

DRAFT AGENDA

Zurich, 12-13 May 2017

Contacts: Elettra Ronchi: Tel: +33-1 45 24 18 28; e-mail: elettra.ronchi@oecd.org
Claire Hilton: Tel: +33-1 45 24 76 91; e-mail: claire.hilton@oecd.org

JT03413623

Complete document available on OLIS in its original format

OECD EXPERT WORKSHOP ON

IMPROVING THE MEASUREMENT OF

DIGITAL SECURITY INCIDENTS AND RISK MANAGEMENT

TAKING STOCK OF PROGRESS AND PRIORITIES FOR INTERNATIONAL ACTIONS

12-13 May, 2017

Swiss Re Centre for Global Dialogue. Gheistrasse 37 8803 Rüschlikon Switzerland

Background

1. Participation in the digital economy allows businesses to increase productivity and expand their market. At the same time it raises new security and privacy challenges as a result of the fast pace of technological innovation and increasing interdependencies between networks and the operations of infrastructure and businesses.

2. The perceived risk related to cybercrime and digital security incidents moved into the top five global business risks in 2015 (in 2014, digital security risks ranked 8th and in 2013 just 15th), according to the fourth annual Allianz Risk Barometer Survey[1]. In the World Economic Forum's Global Risks 2015 report, digital security risk was perceived as a major risk in terms of likelihood and impact. It was recognised as one of the top commercial risks along with geopolitics, the environment, and the economy.

3. Digital security risk is a concern that the entire business community shares, but it may have especially serious consequences for smaller businesses. While large business and organisations may have the institutional and financial capacity to develop appropriate digital security risk management, studies in a number of OECD countries suggest that this is not the case for small and medium enterprises (SMEs), and particularly micro-enterprises, which face managerial, skill, knowledge and financial constraints. The dearth of reliable evidence on which to base digital security risk management decisions and public policy actions compound these challenges.

4. While the frequency and severity of digital security incidents has grown, our ability to measure, analyse, understand and manage them efficiently has not kept pace. A long standing problem has been the lack of consensus on definitions, typologies and taxonomy, as well as a paucity of historical data on "digital security incidents, threats and vulnerabilities". In addition, the limited data sharing that has taken place has failed to spur the development of broadly accessible digital risk actuarial data needed to advance the digital security insurance market more comprehensively.

5. The development of a more reliable and comprehensive data set on digital security incidents and digital risk management practice would likely require:

(i) consensus on typology and taxonomy ;

(ii) trusted public-private digital security incident repository;

(iii) incentives (e.g., mandatory notification requirements) to promote reporting of incidents and data sharing by organisations.

[1] http://www.agcs.allianz.com/about-us/news/press-riskbarometer2015/

6. There are today a number of different fora and initiatives by government, academia, insurance companies and other private sector stakeholders aimed at addressing how to meet these requirements.[2] The value proposition of a data repository for information on digital security incidents, including possible data requirements and system attributes is also being discussed by insurance companies and government in a number of countries (United States, United Kingdom, France).

7. The OECD has started to examine these various initiatives as part of its work on improving the evidence base on cybersecurity and privacy policy-making following the 2016 Cancun Ministerial on the Digital Economy. These issues have also arisen in the context of an OECD project on the cyber insurance market given the constraints that limited data availability have imposed on the development of the cyber insurance market. This multi-stakeholder workshop aims to further take stock of progress to date, examine how the private and public sector can jointly address the challenges, and advance this work.

8. Specifically, the objectives of the Workshop are to:

- **Address Data Collection and Sharing Challenges:**

  What are the main measurement needs? What can and should be measured?

  What typologies, frameworks and standardized approaches are likely to foster useful data collection and reporting for businesses, insurers and policymakers?

  What can we learn from the insurance sector?

  Is there a business case for a digital threat, vulnerability, incident and impact data repository? If yes, at what level (international, regional, national, local, industry-specific, etc)?

- **Examine the range of incentives or mechanisms that can be applied to influence the reporting and sharing of data and their impact on digital security risk management practices in businesses**

  What policy levers can be used to promote greater digital security incident reporting and sharing?

  What are the challenges and opportunities of mandatory disclosure obligations for companies relating to digital security incidents?

  Can minimum requirements for coverage under digital risk insurance play a role in promoting good digital risk management by businesses? How should they be developed, implemented and evaluated?

  How can policy and insurance jointly play a role in raising awareness, developing skills and incentivising good digital risk management practice in businesses?

  What are the most promising areas for future research and policy action?

[2] These include, for example, recent efforts by the UK Department for Business Innovation & Skills, the US Department of Homeland Security Cyber Incident Data and Analysis Working Group, the French public-private initiative led by IRT-SystemX, the Cambridge Centre for Risk Studies, the CRO Forum (representing chief risk officers of large multinational insurance companies) and the Geneva Association.

OECD EXPERT WORKSHOP ON IMPROVING THE MEASUREMENT OF DIGITAL SECURITY INCIDENTS AND RISK MANAGEMENT:

TAKING STOCK OF PROGRESS AND PRIORITIES FOR INTERNATIONAL ACTIONS

DRAFT AGENDA

12-13 May, 2017

Venue: Swiss Re Centre for Global Dialogue. Gheistrasse 37 8803 Rüschlikon Switzerland

Friday, 12 May **16:00-18:30**
Registration will open starting from 15:00
Session I ***Opening of the meeting and setting the scene (16:00-18:30)*** *Welcome remarks by Swiss authorities and OECD Secretariat will be followed by keynote presentations*
Managing Digital Security Risk: Defining the Challenges *(16:00-17:15)* *Jordana Siegel Director, International Affairs* *Office of Cybersecurity and Communications (US) (tbc)* *Robert W. Gordon, Executive Director, Canadian Cyber Threat Exchange (Canada)* ***Measuring and modelling cyber risks - how the private and public sector need to address the challenges*** *(17:15-17:45)* *Matthias Weber, Group Chief Underwriting Officer Swiss Re* ***Title to confirm*** *(17:45-18:15)* *Marc Henauer, Head of MELANI Program. Swiss Federal Intelligence*
18:30-21:00 **Cocktail and Dinner**

Saturday, 13 May

08:30-17:30

08:30 – 08:45

Opening of the Meeting and welcome

Session II:

Digital Risk Management:

How can we overcome the data collection and risk measurement challenges?

08:45-09:15

Key Note: Digital Security Risk: What do we know? What can we measure?
What are the primary barriers to collection and sharing of digital incident and loss information?

Martin Eling, Director of the Institute of Insurance Economics, University of St. Gallen

Followed by Q/A

Panel I: Addressing Key Data Collection and Sharing Challenges

09:15-10:30

What frameworks and standardised approaches are likely to foster useful data collection and reporting for businesses, insurers and policymakers?

Panellists

- *Benjamin Dean, OECD Consultant - Results of an OECD Study on Digital Risk Management Practices in Business*
- *Nicholas Kitching, Head Risk Management EMEA for Reinsurance - CRO Forum Categorization Methodology for Cyber risk*
- *Eireann Leverett, Senior Risk Researcher, UK Cambridge Judge Business School - What language do CERTs need to speak to interact efficiently with insurers?*
- *Leigh Wolfrom, OECD Policy Analyst - Results of an OECD Study on Supporting an Effective Cyber Insurance Market*

Followed by Discussion

Key Note: Public-Private Partnerships for Improved Data Collection and Sharing (10:30-11:00)

Dr Shaun Wang Director, Insurance Risk and Finance Research Centre (Singapore)

Coffee break

11:00-11:30

Panel II: Challenges and Opportunities of incident disclosure obligations

11:30-13:00

What are the challenges and opportunities of disclosure obligations for companies relating to digital security incidents? Can minimum requirements for digital risk insurance coverage play a role in promoting risk management practice? How should they be developed, implemented and evaluated?

Panellists:

- *Kevvie Fowler, National Leader of Cyber Response Advisor, KPMG (Canada)*
- *Hans Allnutt, Partner, DAC Beachcroft LLP (UK)*
- *Mika Susi, Chief Policy Advisor Confederation of Finnish Industries (Finland)*
- *Blair Stewart, Assistant Privacy Commissioner (New Zealand)*
- *Aaron Martin, Vice President Global Cybersecurity, JP Morgan Chase (US)*

Followed by Discussion

Lunch
13:00-14:00

Panel III: Value proposition for a digital security incident data repository

14:00-15:30

What are the opportunities and challenges in establishing a cyber-incident data repository or data-sharing platform? What data can and should be collected (e.g. threats, vulnerabilities, incidents, impacts). At what level might collection be most suitable (international, regional, national, local, industry-specific, etc.)?

Panellists:

- *Steve Bishop, Head of Insurance and Asset Management, ORX (tbc)*
- *Joel Benge, Strategic Communications Specilist (US) - The CyberSecurity Information Sharing Act (tbc)*
- *Yurie Ito, Executive Director Cybergreen (US) - What can we learn from the Cybergreen data sharing platform?*
- *Jerome Notin, General Director, ACYMA (France) – (presentation title tbc)*

Followed by Discussion

Coffee Break **15:30 - 15:45**
Session III **Round -Table Debate and Discussion on Next Steps** **15:45-17:30**
Roundtable Debate: *What are the key lessons to be learnt from ongoing efforts? What are the most promising areas for future research and policy action? How can the OECD contribute to moving the policy agenda forward?* ***Discussion of next steps***
Concluding remarks and end of workshop