Exploring the potential for a “CDC for Cyber”
Informal Davos Follow up Meeting

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Key Issues on the Agenda

What are the key barriers and how are incentives currently misaligned?

Constraints aside, what would an ideal ‘CDC for Cyber’ look like?

What type of information and data needs to be shared to address your business needs?

Which resources would this initiative require?

How can we ensure collaboration among relevant stakeholders?

What creative approaches are there to collectively address these challenges?

May 2013, San Francisco

In January 2013, a group of ICT industry executives and policy makers convened at the Annual Meeting in Davos. The group proposed the creation of a mechanism to share best practices and information about cyber threats. In May 2013, the group reconvened to assess the feasibility of the approach, outline the main barriers, and propose the next steps in moving towards better information sharing and monitoring of threats.

During their discussion, the group focused on two parts: the first part were reasons why a “CDC for Cyber” is not feasible. The second part was aimed at addressing these concerns and finding a common ground to suggest models for a functioning and effective cyber CDC globally.

Part I. Why might “CDC for Cyber” not work?

This part of the discussion addressed the regulatory, legal, economic and organizational barriers to implementing a CDC for Cyber.

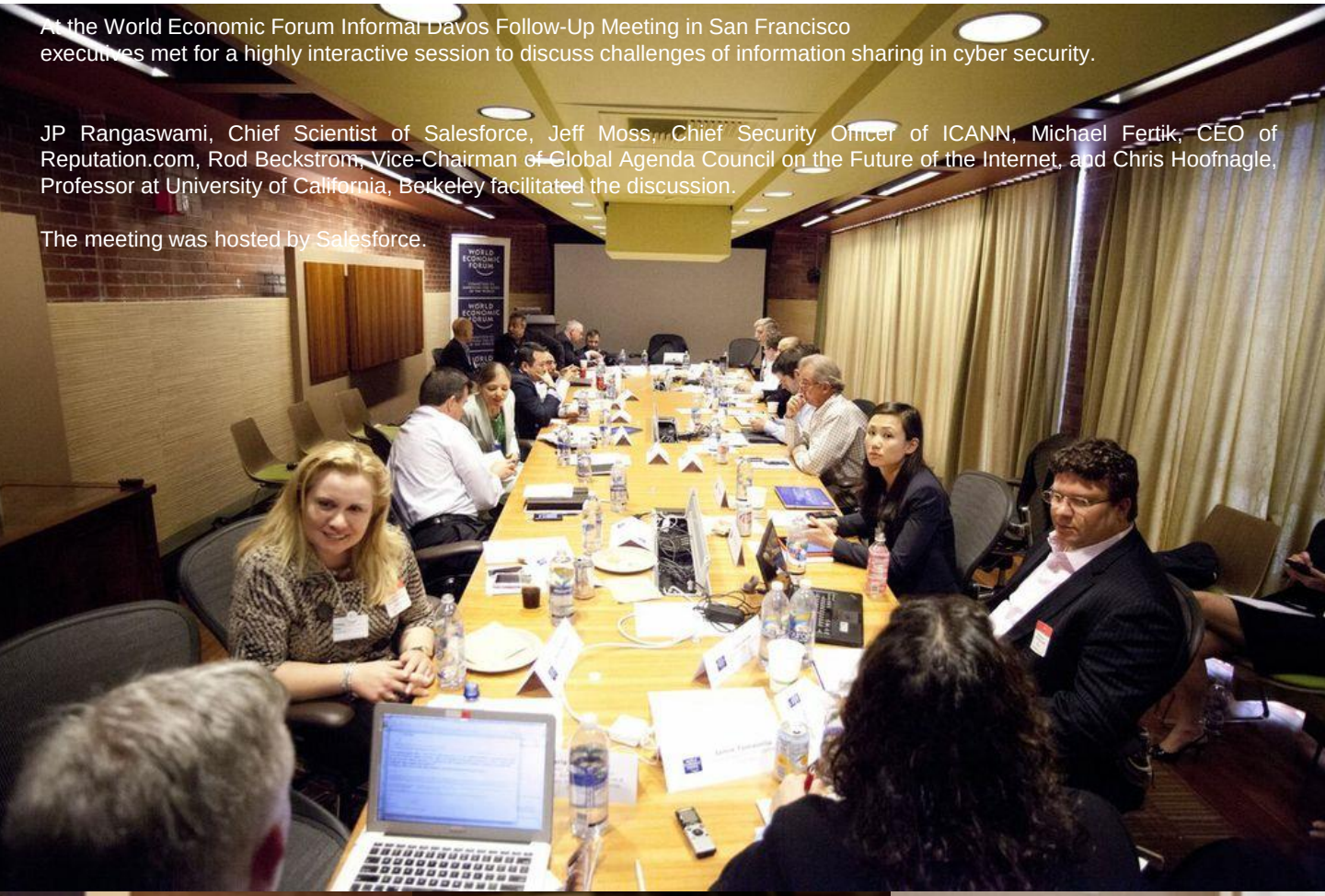
Legal and Regulatory Issues

- Sharing certain kinds of data may be unlawful under current regulations
- Data that companies are willing to share may not entirely belong to them
- CEOs are afraid of legal consequences of sharing data

At the World Economic Forum Informal Davos Follow-Up Meeting in San Francisco executives met for a highly interactive session to discuss challenges of information sharing in cyber security.

JP Rangaswami, Chief Scientist of Salesforce, Jeff Moss, Chief Security Officer of ICANN, Michael Fertik, CEO of Reputation.com, Rod Beckstrom, Vice-Chairman of Global Agenda Council on the Future of the Internet, and Chris Hoofnagle, Professor at University of California, Berkeley facilitated the discussion.

The meeting was hosted by Salesforce.



JP Rangaswami, Chief Scientist, Salesforce

Jeff Moss, Vice-President and Chief Security Officer, ICANN

Michael Fertik, Chief Executive Officer, Reputation.com

Why "CDC for Cyber" may not work?

Lack of security and financial incentives

- Most of the security issues are addressed without CEOs' involvement

Severity

- Level of breaches may not constitute a serious issue in terms of fiscal, brand or other impact
- CIOs do not communicate well enough with the rest of the company about potential consequences
- "High network individuals" who have multilateral relationships across the boards care, can facilitate solutions to information sharing challenges

Centralized approach is counter intuitive

- Centralized problems solving entity may become even a bigger target for attackers
- CDC analogy is not clear: what are the problems that CDC is trying to solve and what role does the information sharing play for CDC?

Trust issues

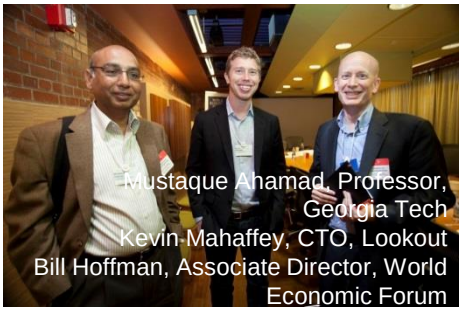
- How can you trust individuals responsible for running the mechanism and other parties that may see the data?
- How do you ensure that the necessary privacy and de-identification measures are taken?

Lack of willingness

- CEOs don't want to share certain kinds of data. The desire to restrain data is more prevalent than to share data
- Market will solve information sharing problems. There exists free market interested in collecting, processing, and monetizing the data

Lack of value

- To address privacy concerns, the data has to be de-identified. The more de-identified the data becomes, the less valuable it is
- Data that will be shared voluntary may not be valuable


Mustaque Ahamad, Professor, Georgia Tech
Kevin Mahaffey, CTO, Lookout
Bill Hoffman, Associate Director, World Economic Forum


Jamie Tomasello, Head of Policy and Investigations, CloudFlare
Chris Hoofnagle, Professor, University of California, Berkeley

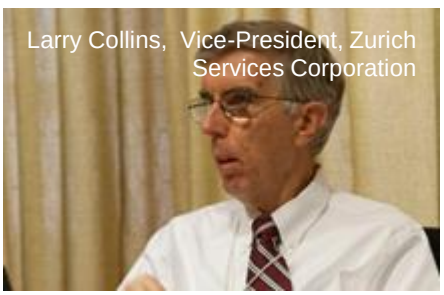

David Ulevitch, CEO, OpenDNS


Lindsey Held, Head, Global Government Affairs, SAP

.


Denise Zheng, Director, CA Technologies


Michael Fertik, CEO, Reputation.com


Larry Collins, Vice-President, Zurich Services Corporation

Why "CDC for Cyber" may not work?

Unclear ownership
- Who will own the data that will be reported?
- What rights will the involved stakeholders have?

Time sensitivity
- Reported data becomes less valuable over time

Lack of focus
- Most information sharing project fail because of the lack of focus on what exactly they are trying to achieve
- What are the classifications and scales of various projects?
- What are the boundaries and definitions of these projects?
- How can you create information sharing if you can't define what the information is that you seek to share?

Increasing scale
- Attacks are growing out of proportion and are becoming too massive to share

Lack of responsible agencies
- What agencies are responsible to take action? Is there a party you can go to if you experience a breach?

Toxic information
- Information itself can be toxic and hazardous and can be misused

Bad history
- Numerous previous attempts have failed. Why go through this again?

Existing competition
- Similar competing initiatives already exist and companies are involved in them . Why


Peter Schwarz, Senior Vice-President, Salesforce
Jeff Johnson, Executive Director, E&Y

Closed groups and free-rider issues
- There is an inherent problem with creating information sharing groups in a setting, such as the World Economic Forum
- How do you include everyone and how do you justify if you exclude someone?

Financial issues
- Who is going to fund the mechanism?

Yuecel Karabulut
Senior Director, SAP


Elena Kvochko, World Economic Forum
Rod Beckstrom, Global Agenda Council on the Future of Internet, World Economic Forum
Sadagopan Singam, Senior Vice-President, HCL
Haden Land, Vice-President and CTO, Lockheed Martin

Part II. What models of information sharing can work?

The second part of the discussion aimed at addressing existing concerns and finding areas for common action among various stakeholders.

Trusted information sharing systems

- "Matchmaking service" approach: very well controlled network, voluntary, private, run by trusted individuals will promote trust
- The participants have to have "skin in the game" and the number of participants should be consistent
- Personal meetings among participants are important for promoting trust
- Importance of semantics in identifying what is shared (default information versus more pejorative)
- Is credit reporting the right model?
- Geographic proximity helps promote trust
- How to deal with the problem of malicious participants in the trust group?

Sustainable economic approaches

- Need to create space for other businesses to benefit from info sharing—allow markets to be created
- Altruism is not enough for sharing
- Need for have mechanisms to address conflicts among participants
- Pooled fund to purchase zero day exploits
- Need collaboration on adversary data


Larry Colins, Vice-President
Zurich Financial Services


Tiffany Rad, Senior Research Scientist,
Kaspersky Lab


Kevin Marks, Vice-President, Salesforce

Government efforts

- DIB Pilot
- DOD exchange on defense contractors about emerging threats
- CERT
- CDC

Places to start

- Report basics of attacks, rather than specifics
- Need to focus upon where people need to share data, narrowly. For example, DDOS is the area where no one is embarrassed to share data.
- Share reported accidents, and in return aggregate stats on costs by kind of incident

MAD models

- Mutually assured destruction vs mutually assured disruption vs mutually assured dependence
- Create models where there is mutually assured dependence
- Share knowledge about bad actors and attack information
- Need to clearly articulate regulations in the way of sharing
- Need models that will work outside the US

If not us, who will do it?

There are many barriers to success of this initiative, therefore, the initial ask from companies and CEOs should be low.

What models of information sharing can work?

The group looked into various models and strategies of information sharing. The group highlighted that there are many barriers to success of this initiative, therefore, the initial ask from companies and CEOs should be low, but oriented towards specific actions.

Rod Beckstrom, Vice-Chairman, Global Agenda Council on the Future of Internet

Patrick Heim, Chief Trust Officer, Salesforce

Next Steps for the Group

- Create a guide on the “10 steps” CEOs should take if there is a breach (create ISO 9000 type of guide)
- Create a list of existing legislative barriers that are in way of greater information sharing. Work together with policy makers to address these challenges
- Encourage CEOs to share attacks attempts
- Write a letter to CEOs on behalf of the group encouraging them to share actionable data and to appoint a person who will own the topic of cyber security. Metrics for sharing such data will be developed by the group.

Additional action items for the group:
•Facilitate peer-to-peer networks and knowledge exchange. Foster a network of practices, protocols and groups
•Encourage CEOs to report basics attacks
•Create an annual report on the Global Network Health with chapter contributions from various companies
•Create a matchmaking service for trusted individuals and experts
•Develop a preliminary concept of information sharing that can be presented at Davos 2014

The group agreed to work together and present the outputs of these efforts during the Annual Meeting of New champions in Dalian, China in September 2013

Jeff Moss, Vice-President and Chief Security Officer, ICANN
Peter Schwarz, Senior Vice-President, Salesforce
Peter Heim, Chief Trust Officer, Salesforce

Creating “CDC for Cyber”
Informal Davos Follow up Meeting

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

List of Participants

- Chris Hoofnagle, Director, Information Privacy Programs, Berkeley Center for Law & Technology, University of California, Berkeley
- David Ulevitch, CEO, OpenDNS
- Denise Zheng, Director, Global Government Relations, CA Technologies
- Donald Proctor , Senior Vice President, Office of the Chairman and CEO, Cisco
- Elena Kvochko, Manager, IT Industry, World Economic Forum
- Eric Openshaw , Vice-Chairman, US Technology, Media and Telecommunications Leader, Deloitte
- Haden Land, Vice-President, Engineering & Chief Technology Officer, Lockheed Martin
- Jamie Tomasello , Head of Policy and Investigations, CloudFlare
- Jeff Johnson, Executive Director for Cyber Security, Ernst&Young
- Jeffrey Moss , Vice-President, Chief Security Officer, ICANN
- JP Rangaswami, Chief Scientist, Salesforce
- Kevin Mahaffey , CTO/Co-founder, Lookout Mobile Security
- Kevin Marks, Vice-President, Open Cloud Standards, Salesforce
- Kevin Sullivan, Principal Security Strategist, Microsoft
- Kevin Wang, Americas CISO, Group Information Security, Zurich Services Corporation
- Larry Collins , Vice President E-Solutions, Zurich Services Corporation
- Lindsey Held, Head, Global Government Affairs Strategy, SAP Labs
- Michael Fertik , CEO and Founder, Reputation.com
- Mustaque Ahamad, Director, Georgia Tech Information Security Center, Georgia Institute of Technology
- Natalia Latimer , Senior Director, Enterprise Strategy, Salesforce
- Parick Heim, Chief Trust Officer, Salesforce
- Paul Royal, Research Scientist, Georgia Institute of Technology
- Peter Schwartz, Senior Vice-President, Global Government Relations and Strategic Planning, Salesforce
- Rod Beckstom, Vice Chairman, Global Agenda Council on the Future of the Internet, World Economic Forum
- Sadagopan Singam, Global Vice-President, HCL Technologies
- Tiffany Rad, Senior Security Researcher, Kaspersky Lab
- Yuecel Karabulut , Senior Director, Security Engineering, SAP Labs

For questions about the initiative, please contact Elena Kvochko, Manager, IT Industry elena.kvochko@weforum.org