WORLD ECONOMIC FORUM

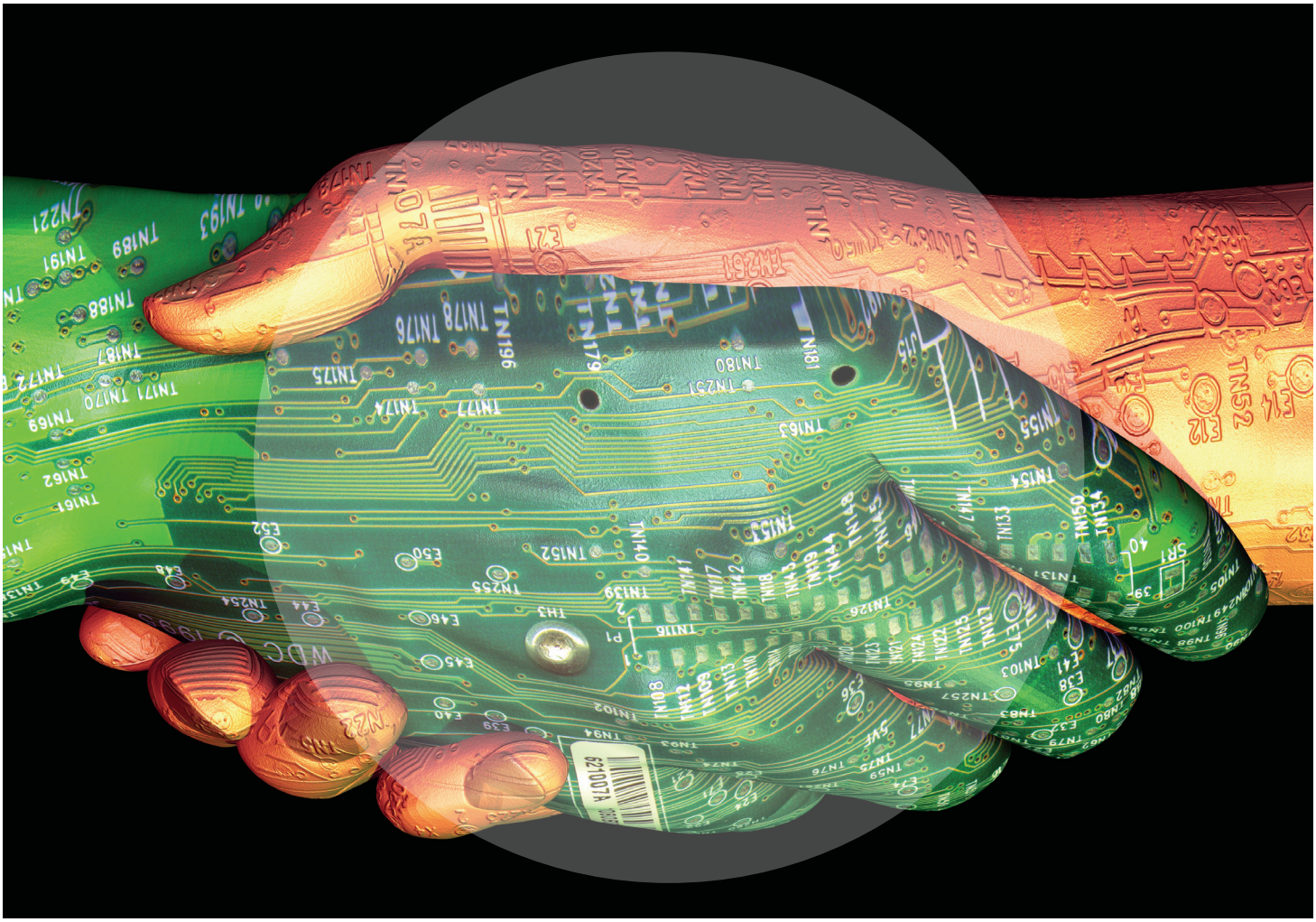
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

Partnership for Cyber Resilience

Newsletter

December 2013



REF 101213

Contents

Partner Roundtable

McKinsey hosts financial services CISOs

As part of the World Economic Forum's Partnership for Cyber Resilience Initiative, McKinsey & Company hosted on 17 October 2013 chief Information security officers from 15 of the world's largest financial institutions to discuss the largest threats to their businesses from cyber attacks. Of the institutions represented, most have experienced at least some type of attack with varied levels of success.

The following points were raised:

1. There is growing acceptance about the level of connectivity involved in daily operations of each part of their organizations; no single system operates in isolation. As this level of interconnectivity increases, so does the level of interdependence with systems, both internally and externally. This mutual dependence means that each organization has a responsibility to interact with and improve the general state of the environment.
2. As the threat increases, so too will the need for resources to combat such threats. However, the amount of spending does not necessarily translate into maturity. Rather, there needs to be some valuation of the ROI from cyber-related spending; that amount would not be 100%.
3. Advanced analytics are needed to keep pace with the ever increasing maturity from potential attackers. There is a sense that the sophistication of attackers is increasing dramatically in most cases. To keep pace and to monitor potential threats, advanced analytics are going to be needed, which may or may not exist today.
4. Defining the effects that cyber threats are having on businesses compared to other risks are a challenge due to the lack of an appropriate way to measure the impact. A true game-changer would be the ability to quantify the risk of cyber attacks and cyber threats.

Leaders Sign Forum's Cyber Resilience Principles

At The Grand Conference 2013 – held in Amsterdam on 5 November – participants had the opportunity to sign on to the World Economic Forum's Principles for Cyber Resilience, showing their commitment to improve the resilience of their internal and external digital infrastructures. Supporting the Forum's Partnership for Cyber Resilience initiative, of which the Principles are a part of, is a clear step in developing public-private participation, one of the key pillars of the new Dutch Cyber Security Strategy.

Ivo Opstelten, Minister of Security and Justice of the Netherlands and the national policy coordinator for cyber security, signed the Principles in the presence of Eberhard van der Laan, Mayor of Amsterdam. They were joined by Chris Buijink, Chairman of the Dutch Association of Banks (NVB), Bart Hoogendoorn, Chairman of Nederland ICT, Rob Wainwright, Director of Europol, and Udo Helmbrecht, Executive Director of ENISA.

As part of the signing ceremony, Jan Mengelers, Chairman of the Board of Directors of TNO, and Kevin Kalinich, Global Practice Leader for Aon, spoke on why they had already joined the initiative earlier this year. Jacques Buith, Managing Partner Deloitte, which supported the Forum in developing the initiative, also discussed the impact of the Principles.

By signing the Principles for Cyber Resilience, chief executives and government ministers join a growing group of leaders that form the Partnering for Cyber Resilience initiative. Although the Principles are not legally binding, they reflect an organization's commitment to corporate governance best practices in a digital, connected world.

The Grand Conference also served as the venue for the official closing of Alert Online, the Dutch cyber security awareness campaign. As part of the campaign, partners from industry and government worked together to boost cyber security awareness in the Netherlands.

01

01: Udo Helmbrecht, Executive Director, European Network and Information Security Agency (ENISA), Athens, and Rob Wainwright, Director, Europol (European Police), The Hague

Interview with HP Executives on Cyber Threats

Interview with Art Gilliland, Senior Vice-President and General Manager, Enterprise Security Products, Hewlett-Packard, and Jacob West, Chief Technology Officer, Enterprise Security Products and Head of Security Research, Hewlett-Packard

Cyber threats are increasingly being perceived as an overall business risk issue, rather than a technical problem. Do you agree with this statement and how do you think the nature of cyber threats is changing?

Art Gilliland: Over the past five to seven years, cyber attackers have changed their philosophy. Today, it is less about breaking in to disrupt technologies or get visibility and credibility with the "bad guys", and much more about gaining access to intellectual property or for economic gain. What it means from the business perspective is the need to protect your valuable assets. CEOs and board of directors are paying more attention to cyber risks. Companies are no longer competing with the individual hackers, but with a market ecosystem.

Jacob West: We are also seeing increased level of rigor and science on the adversary side. The fact that we have developed the vocabulary for talking about security and defence capabilities has made it easier to discuss these topics with broader audiences and get security on the boardroom agenda. Efforts, such as creating maturity models, help us measure the necessary investments and, therefore, better plan for the future. We are also collaborating with the community of peers on the defender side to share best practices, compare investments and get more scientific about dealing with what used to be "black art".

Do you think enough of the CEOs and boards are already paying attention to cyber threats and if not, what can be done to improve the situation?

Art Gilliland: The boards and the CEOs, especially at large companies, are paying attention to the issues of cyber threats. Most of them have security audit committees. Part of what has driven the attention is regulatory and policy standards or frameworks, such as ISO 2700 or 2701. The awareness about security is at a much higher level today. However, medium to small and private companies don't have the same level of pressure and need more awareness as they continue to be the target.

Policies and standards can be seen as a double-edged sword. On the one side, they show where the organizations need to be and help raise capabilities of the industry as a whole. On the downside, they create aspirations to reach that low bar. It is not enough to think "If I do these things, I will be safe". In fact, if you do these things, you will be as good as the worst player on the industry. As an industry, we have to be more thoughtful about how we are disrupting the adversary process.

Jacob West: Cyber security shifted from art to science. We see an increasing level of maturity in the nature of the conversation, where we talk about what is the responsibility of a modern enterprise today when it comes to security and how they can fulfil this responsibility without needing the latest breach to motivate them.

Art Gilliland: We have to start focusing beyond the check box towards more effectively stopping the adversaries, protecting our assets and mitigating the risks.

What is your advice on how to increase the maturity level of the conversation around cyber threats and to better manage risks at an enterprise level?

Art Gilliland: It is important to separate protection and security policies from mere compliance. Compliance is different from stopping the adversary. Executives need to understand stages of a breach and the capabilities they have to build to disrupt the adversary process. We distinguish five levels in the attack lifecycle:

1. *Research* – Adversaries try to build profiles about our people and the environment
2. *Infiltration* – They use these profiles to target us through social engineering and other ways
3. *Discovery* – Adversaries use access points to create internal map or sensitive assets
4. *Capture* – They capture the information they care about
5. *Exfiltration* – They take out the information and sell it or use for other purposes

Enterprises need to build capabilities to counter these five steps, not only to stop adversaries, but to locate them after they break in and to protect the assets and limit the damage. This should be practiced, like fire drills.

The applications that we are developing are for global protection. Speaking a common language internationally will make us even better. Moreover, cooperation between law enforcement and government agencies will help us build better and more consistent policies. Another area that I would like to draw attention to is addressing the skills gap, as demand for and supply of security expertise is very unequal.

Jacob West: We are already seeing limited collaboration within the industry through groups like FS-ISAC and the World Economic Forum. Some of the sharing will happen at the technical level. Equally valuable are at the governance and project management levels. Collaborative response is a lesson we can learn from adversaries themselves. We encourage our partners not only to distinguish compliance with capabilities, but also augmenting the skill sets. We will continue to invest in security research. We have begun a series of security briefings to highlight key areas of security research and profile best practices.

Interviewed by: Elena Kvochko, Partnership for Cyber Resilience Lead

Highlights from the OAS Regional Cyber Security Symposium

The Organization of American States (OAS) hosted a regional cyber security symposium in Montevideo, Uruguay, on 11-13 November 2013 in partnership with the World Economic Forum's Risk and Responsibility in a Hyperconnected World initiative. The symposium brought together representatives of government and the private sector from over 20 nations across the Americas.

The three-day symposium covered a variety of topics, including considerations for the development and implementation of national cyber security strategies and national awareness raising campaigns. Some of the overall points discussed included:

- Cyber security is highly correlated with the increase in quantity and sophistication of cyber crime
- There is an imperative for a legal framework to establish rules and protocols for dealing with cyber crimes and which establish roles and responsibilities for different agencies
- There are varying levels of sophistication within the region and there is an opportunity to share these best practices inter-regionally
- There needs to be increased public-private cooperation, especially given the often tenuous relationship that currently exists in this space

Recommendations:

- Any national strategy needs to be highly dynamic and flexible to react to the ever changing structure and variation of attacks
- It is not enough to develop a national strategy; nations need to ensure that strategy translates into effective policies for government and the private sector
- An effective information sharing platform must be a core component of any national strategy
- The end goal should be to foster an environment of trust and transparency among all stakeholders

During the symposium, participants also discussed such issues as national governmental coordination, fostering collaboration of relevant stakeholders and incident response capabilities.

Task Force Meeting on Measurement and Quantification of Cyber Risk

EUROPEAN CYBER SECURITY MONTH

One of the key aspects of making better decisions is the ability to benchmark risk levels against known standards and to be able to quantify this risk in non-technical and financial terms. Wipro has volunteered to lead a task force to explore this area and gather views from various industry and government members.

Members and partners of the World Economic Forum's Partnership for Cyber Resilience initiative, including
Wipro, Aon, BP, the Cabinet Office of the United Kingdom, CA Technologies, ENISA, ISF, Shell and Unilever, met in a workshop on 13 November 2013 in the UK to address measurement and quantification of cyber risk.

Main discussion points:

- There is a need to be able to conduct the exercise in a relatively short period of time and provide indicative benchmarks; the benchmarking is not meant to be a rigorous audit exercise
- Some benchmark data around the level of risk and security posture would enable organizations to better understand how they feature vis-à-vis peers and make a decision based on their risk tolerance
- Finding the relevant assets might be an art
- Boards will mature over time regarding cyber awareness; initial conversations are needed to sensitize them while subsequent conversations would focus on monitoring the current threat posture, possible risks and hence specific actions that need to be conducted

There is a need to measure and articulate cyber risk in a holistic, preferably monetary form. To be credible to boards and to avoid getting into debates on the exact value, parameters of relevance and ranges of economic impact should be defined. The following actions should be taken:

- Include security auditors and insurance underwriters to provide feedback around how useful this exercise could be in their activities.
- Include the academic community once the scope of the initiative and its boundaries are defined more clearly
- Conduct a similar workshop in the US to solicit similar feedback and create a common view that could be driven through the next year
- Drive periodic conversations to gather momentum behind this effort; tentatively planned to have monthly calls and another face-to-face conversation in the summer of 2014

European Cyber Security Month

Connecting the Nodes and Participation for Assuring Online Security

By Daria Catalui, European Union Agency for Network and Information Society (ENISA)

The EU Cyber Security Strategy calls for an open, safe and secure cyberspace, including raising awareness as a common responsibility. This is being put in practice in a yearly European Cyber Security Month advocacy campaign deployed currently in 27 countries. More than 40 public and private stakeholders are supporting the Cyber Security Month, including the EU cyber security agency ENISA, the European Commission and Vice-President Neelie Kroes, and the Directorate-General CONNECT.

Sharing of experiences and further recommendations were exchanged in a kick-off event on 11 October. Participants discussed how digital citizens can more effectively become engaged and how to measure the impact and which performance indicators to include. These issues will be further explored in an evaluation report to be published in November.

The role of ENISA in the campaign is to be a broker of information, give support for stakeholder mapping and participate in the building of public-private partnerships. Support at the European level makes the work more efficient and builds up a strong NIS community behind the campaign. This role is central in advocacy.

Additionally, the concrete activities that bring added value happen most of the time at local level, with public bodies, private stakeholders, professional associations and citizens, all working together for greater cyber security in today's digital environment. All these sustained efforts aim to create active involvement in the promotion of cyber security for citizens, placing the topic firmly on both agendas for citizens and governments.

Calendar of Events

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. The calendar is updated regularly and available for download here.

	December 2013	January 2014
Forum-led events		**Annual Meeting 2014** Davos-Klosters, Switzerland 22-26 January
Project Dialogues	**PCR Working Group Meeting** Brussels, Belgium 5 December **PCR Working Group Meeting** Washington DC, USA 12 December	

Partners

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

Contact Information

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

Elena Kvochko
Partnership for Cyber Resilience

cyberresilience@weforum.org

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.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org