Cyber Resilience in the Board Room

Marieke Klaver
TNO
marieke.klaver@tno.nl

Annemarie Zielstra
CPNI.NL
Director
annemarie.zielstra@cpni.nl

The Grand Conference - Building a Resilient Digital Society - took place in Amsterdam on October 16, 2012. The international conference aimed for top decision-makers of industry government and other organisations. Two hundred participants from twenty-two nations participated. Three Dutch organisations showed leadership during the conference and signed the World Economic Forum principles for Cyber Resilience; and hope to stimulate other organisations to join as well.

'The Grand Conference' was organised by the Dutch Centre for the Protection of the National Infrastructure (CPNI.NL) in close cooperation with the European Commission, the European Network and Information Security Agency (ENISA), the US Department of Homeland Security (DHS) and the World Economic Forum (WEF). The conference was an outreach of the EU-US Working Group on Cyber Security and Cyber Crime. This working group covers information exchange, knowledge sharing and cooperation on the domains Industrial Control Systems (ICS) security and Smart Grid security. ICS are critical components which monitor and control the functioning of most of our critical infrastructures, e.g., the power grid, drinking water, automated food processing, and tunnel safety. Smart Grid is the development where information and communication technologies, ICS and the traditional energy (and other) grids are integrated to improve the reliability of supply and to reach the green European 20-20-20 goals. Therefore it is of the utmost importance to society that ICS and Smart Grids are robust against cyber disturbances including cyber-attacks. Dependencies between (critical) infrastructures, value chains and dependencies between organisations require a shared cyber security responsibility which ask for cooperation between nations, governments, government agencies, private parties, manufacturers and users of these systems.

The conference highlighted different aspects of the creation of a secure and robust digital society: opportunities of the increasing connectivity, via threats, to solutions such as risk management, organisational strategies and the use of economic incentives to reach cyber resilience.

The conference was opened by Annemarie Zielstra, director of CPNI.NL. Harry van Dorenmalen, chairman of IBM Europa, presented an optimistic future about the role of information and communication technologies in 2030 and the chances for society. Mikko Hypponen, Chief Research Officer of F-Secure, sketched the dark side of cyberspace and outlined the many actors which try to abuse the increased interconnectivity of organisations. According to him, the largest threat is state-sponsored attacks. It will be a hard for organisations to defend against a "James Bond" with USB-sticks as part of the M-supplied armour package. Mike Maddison (Deloitte), Rod Beckstrom (previously CEO of ICANN) and professor Michel van Eeten (TU Delft) discussed the solution directions mentioned above. In the afternoon, master classes were scheduled on risk management for ICS and Smart Grids, crisis communication and reputation management, and ICS Security for managers. A live demo hack by the golden CyberLympics team of Deloitte impressed many of the conference attendees.

The World Economic Forum (WEF) was one of conference partners because of the large global economic interest that cyber security poses. The WEF stimulate organisations to continuously address the topic cyber resilience in their board rooms as a resilient cyber posture is crucial to operate in a ‘hyperconnected world’. The WEF manifest “Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines” is a tool to support the C-levels of organisations in understanding their level of cyber resilience (reference 1).

The four WEF principles are:

- The organisation recognizes the interdependent nature of our hyperconnected world and its own role in contributing to a safe shared digital environment.
- The executive management team recognizes its leadership role in setting the tone and structure for cyber resilience.
- The organisation recognises the importance of integrating cyber risk management within its broader risk practices and in line with these Principles and Guidelines.
- The organisation encourages its suppliers to adopt these Principles and Guidelines.

Signing ceremony of WEF principles
Partnering for Cyber Resilience
Mr. Derek O'Halloran
World Economic Forum

The WEF promotes this manifest as a means to initiate the cyber resilience dialogue in organisations and to render the board room commitment permanently. During the conference, C-level representatives of Alliander, KPN and TNO showed leadership by publicly signing the WEF manifest.

Finally, Mark Dierikx, Director-General of the Dutch Ministry of Economic Affairs, underpinned the interest of his department in a reliable and resilient cyber infrastructure. The closing speech was by Mrs. Kroes, Vice President of the European Commission and responsible for the Digital Agenda. Mrs. Kroes made the point that there is an increase both in number and seriousness of cyber incidents. For that reason, the European Union is increasing its efforts on Digital Security by launching a European Cyber Security Strategy later this year. The strategy includes the need for international cooperation between the EU member states. The ICT infrastructure and cyber attacks aimed at them do not stop at national borders. The European Commission therefore aims to increase the level of digital protection in all EU member states. She stated that the cyber security cooperation between critical infrastructure operators (e.g., energy, transport, telecommunication & IT) is an essential element of the strategy. Public and private parties need to collaborate jointly, each party taking his responsibility.

Regarding responsibility, Mrs. Kroes remarked that this does not stop at corporations and governments. Each ICT user has responsibilities for a secure cyberspace. Simple measures may make the difference, therefore the EU has appointed October as European Cyber Security Month in order to include the home users in the cyber security discussion. Last but not least, Mrs. Kroes state that international cooperation with nations outside the EU is key to the strategy: “It's time to give cyber-security the attention it deserves. Let's be strategic, let's work together, and let's ensure we protect our infrastructure, and our citizens, in the digital age.”

One of the key agenda elements of the conference took place during the evening. An exclusive party of some forty top executives were challenged during a walking dinner with three future scenarios. They worked together to create a cyber security network at the board room level and to provide inputs to the WEF meetings in Dublin and Washington (December) and the yearly WEF conference in Davos (January 2013). It became obvious that showing leadership at the top of organisations is crucial to increase the digital resilience of our society. The government should facilitate, stimulate and take away impediments for the private parties. The Grand Conference was a first step to structural discussions between public and private parties about cyber resilience and the road ahead.

The conference will be a major success when actions are made concrete and lead to an increased commitment for cyber resilience in the board room. One success can be noted. The European Commission will support the organisation of a subsequent conference in 2013: The Grand Conference 2013.

You and your organisation can act now!

Under reference 2 you will find more information on cyber resilience: a set of awareness material, a database with critical infrastructure disruption incidents, and a C-suite executive checklist based on the WEF principles. The checklist helps you to determine the cyber resilience maturity level of your organisation in relation to other organisations. During the conference, the participating organisations scored above average for their own resilience. However, when it comes to their supply chain, a less mature result emerged. You are encouraged to determine the maturity level of your organisation by using the tools and to take action to raise your digital resilience when required.

References

1. World Economic Forum, Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines, on-line: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.
2. See: www.cyber-resilience.org

Securing European Smart Grids

ENISA's Recommendations

Dr. Evangelos Ouzounis
ENISA
Head of Resilience and CIIP Unit
www.enisa.europa.eu

Dr. Konstantinos Moulinos
ENISA
Smart grid security programme manager
www.enisa.europa.eu

The smart grid can be defined as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added.

Smart grids will be able to efficiently integrate the behaviour and actions of all users connected to it — generators, consumers and those that do both — in order to ensure an economically efficient, sustainable power system with low losses and high quality and security of supply and safety.

Information and Communication Technologies (ICT) are envisioned to be the underpinning platform of the smart grids, which exemplifies the increasing dependency of European economy and society on communication networks and computer applications.

Achieving a secure smart grid will not be an easy task. Assessing risks, securing processes as well as identifying technological gaps and organizational problems are some of the main challenges that the smart grid will face in the years to come. Raising awareness and fostering training and knowledge sharing among all the actors are urgent measures needed to set the breeding ground for bringing security to the first line of action.

European Policy Context

In 2009, the Commission adopted COM(2009) 149[1] on Critical Information Infrastructure Protection. This Communication recognizes that ICT infrastructures are the underpinning platform of other CIs and defines a plan of immediate actions to strengthen the security and resilience of Critical Information Infrastructures (CIIs) based on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, and criteria for EC infrastructures in the field of ICT. In 2011, another Communication from the Commission, COM(2011) 163[2], summarised the achievements of this plan and defined next steps to be taken. It also recognized that new threats have emerged, mentioning Stuxnet as an example. Besides, this Communications specifically mentions that Smart Grids can be affected by sophisticated and targeted cyber threats, with disruption-purpose.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF