SAFEGUARDING THE DIGITAL ECONOMY

B20 COALITION RECOMMENDATIONS ON IT SECURITY TO G20 GOVERNMENTS

Issued on: 30.07.2015
The B20 Coalition has made the Digital Economy its priority for 2015 and has identified three areas of action, to start with:

**IT Security** – because it is one of the biggest concerns in implementing the digital agenda;

**Global Standards** – because in an increasingly interconnected world the base cannot be built upon without common standards; and

**Smart Cities** – because our future lies in making our cities more sustainable, efficient and responsive.

To report on the main challenges identified by the companies that it represents, the Coalition’s digital agenda was introduced in June 2015 with the publication of a series of recommendations to the G20 governments – *Digital Economy: The Driver for Growth*.

Finally, with the goal of fostering the integration of Digital Economy into the G20 leaders’ agenda, the B20 Coalition has committed its network in co-organizing with B20 Turkey, a conference on digital economy, called *The Third Wave: Digital Economy and The Industrial Internet*. This first-of-its-kind initiative will take place on October 06, 2015, in Istanbul, in parallel to the G20 Trade Ministers’ meeting.
CONTENTS

- Abstract .......... 4
- Introduction ........ 5
- IT Security Challenges .......... 6
- B20C Recommendations .......... 8
  - Strengthen Trust for the Future of Digital Solutions .......... 8
  - Strengthen International Cooperation Between Public Authorities and Between Public & Business Sectors .......... 9
  - Establish Data Protection and Data Security for Cloud Computing .......... 10
  - Improving Standards & Norms to Increase IT Security .......... 12
  - Strengthen Prevention through Education .......... 13
Abstract

The digital transformation of the economy offers great opportunities. Business and consumers can benefit from a wider range of products and services, lower costs and higher efficiency levels. Innovative products and new competitors along with an unprecedented potential for market penetration can preserve growth and prosperity worldwide. Digital global value chains will foster future growth and will become the next key driver of global integration. Nevertheless, the facilitation of secure and reliable data is a mandatory prerequisite in order to leverage the existing potential. This has already become a truly global challenge. Therefore the B20C examines four major recommendations.

The G20 must strongly act against organized cybercrime since digital solutions suffer from a severe loss of confidence.

Furthermore, public authorities and business must work closely together to enable dynamic global security measures.

Thirdly, in regard to the future establishment of digital environments it is of great importance to secure cloud computing systems. The G20 should expand international cooperation on standards and norms since they play a key role in improving cyber security and cyber defense.

Finally, it is important to strengthen the sensitivity of users, companies and governmental bodies towards cybercrime.
INTRODUCTION

The leading independent industry associations and business organizations from G20 countries – the B20 Coalition – will pay special attention to the digitalization of the economy in 2015.

The B20C strives to address the global impediments to the digitalization of the economy as well as to outline potential strategies towards a digital future.
Digitalization of the economy is borderless and disruptive at the same time. It brings about radical change at a breathtaking pace. Internet, mobile communication and digital applications provide great opportunities to develop new business models and market strategies. This is particularly true for innovative small and medium-sized enterprises.

Moreover, the “Internet of Things” will tremendously change the traditionally industry-led processes. Interconnected “smart” factories will be able to control autonomous global production and supply chains. Intelligent trading hubs will independently distribute products and commodities.

Smart services and digital applications will provide highly individualized products and services for end-consumers. These interconnected digital ecosystems will be highly dependent upon the exchange of information.

Available and comprehensive quantities of data form the backbone of the digital revolution. Market participants analyze and transform data sources into “smart-data” fitted to their economic requirements.

Only the use of reliable smart-data enables market participants to develop innovative services and to increase the efficiency of industrial processes. Smart-data allows for the evaluation of economic decisions and possible outcomes faster and
more accurately. Research and innovation cycles will be simpler and quicker. Reliable and high-quality data are key to the success of the digital future.

It is expected that around 6.5 billion people will be interconnected with at least 18 billion objects in 2020. Thus, it is likely that today’s data volume will increase tenfold by 2020.

As more consumers and business companies become dependent on the digital ecosystems, the cost of cybercrime and regulatory shortcomings will increase extensively. Losses from viruses, sabotage, industrial espionage, and theft of intellectual property are likely to become a structural impediment to the digital solutions. Current studies estimate that the impact from cybercrime was around 0.5 per cent of GDP on average in 2013.

Therefore, the quality and security of data will be of fundamental importance to the digital future. The security of IT systems is a prerequisite to exploiting the considerable potential of the Digital Economy. Without trust, consumers and business will be reluctant to welcome digital solutions.
B20C RECOMMENDATIONS

Strengthen Trust for the Future Success of Digital Solutions

Criminal organizations are attacking digital environments with increasingly professional methods. Data are stolen, manipulated or spied on without the owner’s knowledge. Technical systems are sabotaged and intellectual properties are stolen. The losses within companies add up to tens of billions of euros.

Digital solutions suffer from a severe loss of confidence, particularly, now that the practices of intelligence services have been revealed. However, without trust in innovative applications, consumers will be reluctant to accept digital solutions.

The B20C outlines the necessity of ground rules and their enforcement. The G20 must act strongly against organized cybercrime.

Reliable data protection as well as strong data security – properly implemented and enforced – must focus on a more transparent, dynamic and consumer sovereign approach. It is important to facilitate flexible approaches for businesses to adopt cyber security standards. It is crucial to protect the flow of knowledge and to reinforce the right to determine how information is used.
Strengthen International Cooperation Between Public Authorities and Between Public & Business Sectors

The security of the digital environment must be regarded as a procedural process. It is important that new developments are considered in their entirety in order to secure the potential of digital markets and value chains.

Stakeholders from state, industry and society should cooperate more closely to further improve and coordinate existing frameworks and regulations. All stakeholders should jointly develop ambitious global framework conditions.

Thus, it is important to enhance public-private cooperation and to strengthen information sharing processes on a voluntary basis. It is essential that these initiatives are able to foster different private sector innovations in the area of security. Furthermore, as cybercrime does not recognize any national borders, the B20C encourages national security bodies to work closely together and to improve their coordination.

With regard to investigations and sanctions of criminal organizations, the G20 should enhance mutual administrative assistance treaties. Cyber security should be more deeply embedded in global discussions. Therefore, it is important to initiate an appropriate forum for all stakeholders with an equal footing. Furthermore, initiatives at the national level must be designed consistently in order to improve compatibility in the international context.
Moreover, due to businesses having strong incentives to provide a secure digital environment, the B20C supports global networks of all stakeholders on a voluntary basis. Since IT security lays the groundwork for future investments and growth, business will strongly contribute to institutionalized private and public security networks.

Examples like Computer Emergency Response Teams (CERT) already point in the right direction. CERT is an organization that handles security incidents in the framework of CERT activity. CERT organizations exist worldwide and they cooperate closely, exchange information about security incidents and hazards, as well as existing best practices.

**Establish Data Protection and Data Security for Cloud Computing**

The dissemination of cloud computing offers great opportunities. It uncouples IT capacities from local computers to a central unit. The storage of information and the use of software can therefore be offered individually and dynamically. Cloud computing extensively increases companies’ and users’ flexibility and efficiency. It will enable new business models and enhance future growth, especially for Small and Medium Enterprises (SMEs).

A precondition for acceptance and success is; first and foremost, trust in the integrity and security of these systems. Recent surveys have shown that trust in
cloud systems has considerably decreased due to the latest affairs in intelligence services. These figures are even more worrisome considering that most companies were about to start investing in this new technology.

National markets can only become lead suppliers of cloud services if their security environment is perceived to be reliable and secure. The B20C calls on policy-makers to work towards transparent and coordinated frameworks so that new trust can be generated. Before initiating new security systems it is important that policy makers examine existing policies which apply to cloud computing.

Furthermore, burdens such as high electricity prices or postponed investments in fiber optic cables should not be underestimated. The B20C acknowledges the different policy approaches towards data protection as local advantages. Nevertheless, policy-makers should closely cooperate to create minimum guidelines and to work towards a global level playing field. Therefore, mutual legal assistance treaties as well as the issue of encryption should be further developed.
Improving Standards & Norms to Increase IT Security

Standards and norms play a key role in improving cyber security and cyber defence at the international level. Standardization processes and procedures are essential to achieve effective cooperation in cross-border and cross-community environments. Digital markets and value chains do not recognize national borders. They do not apply to a uniformed legal system and do not have common security or privacy norms.

Nevertheless, digitalization is relatively homogenous in terms of technology. Open and commonly laid standards can improve the efficiency and effectiveness of key processes. Therefore, it is necessary to facilitate the integration and interoperability of security systems globally.

The B20C calls on the G20 to expand the international cooperation on standardization in cyber security. Since cyber security is mostly provided by private sector services, it is crucial to maintain an integrative approach where all stakeholders – private and public – are included.

Furthermore, it is crucial that the G20 agrees on high safety standards compatible with international standards. National exceptions in standardizations should be minimized to implement a global level playing field. Compulsory, auditable minimum standards are needed for the industry.
Strengthen Prevention through Education

The sensitivity of users, companies and governmental bodies towards cybercrime is a core objective to improve IT security.

Only conscious users will pay attention and will be able to initiate effective counter-measures. Therefore, education about risks and prevention must be assured at all levels and in all areas of education. Nevertheless, security will never be absolute, but the hurdles to be surmounted can be lifted.

For example, training employees is a critical element in order to improve IT security. Employees need fundamental knowledge of risks and how to handle them. This will involve putting practices and policies in place that promote security as well as training employees to be able to identify and avoid risks.
This statement is issued in
Berlin, Brasilia, Brussels, Buenos Aires, Istanbul, Johannesburg, London, Madrid,
by the B20 Coalition members

ABOUT THE B20 COALITION

The B20 Coalition brings together leading independent business associations from G20 economies and operates as a worldwide exchange platform between national business communities, aiming at building consensus and developing common positions on critical issues for enterprises.

Through its broad-based representation, the Coalition on behalf of more than 6.8 million businesses of all sizes and from all sectors engages policy-makers on a global scale and advocates policies that contribute to global growth and job creation at regional and international levels. The Coalition is instrumental, notably, in supporting the G20 process and ensuring continuity over successive Country Presidencies.

B20 COALITION MEMBERS

Ai Group, Australia · BDI, Germany · BUSA, South Africa · BUSINESSEUROPE, Europe CBI, United Kingdom · CCC, Canada · CEOE, Spain · CII, India · CNI, Brazil · Confindustria, Italy FKI, South Korea · MEDEF, France · TÜSİAD, Turkey · UIA, Argentina · US Chamber, USA

CONTACT US

Presidency
360 Albert Street Suite 420 Ottawa, ON K1R 7X7

Secretariat
55, avenue Bosquet 75007 Paris France
Email: secretariat@b20-coalition.org

FOLLOW US

on twitter @B20Coalition
on our website at www.b20coalition.org
and join our business community on LinkedIn at B20 Coalition

B20 is a registered trademark of the B20 Coalition
All photo credits Thinkstock