G7 2017 ITALIA

ANNEX 3

G7 ACTIONS FOR ENHANCING CYBERSECURITY FOR BUSINESSES

26 September 2017

OBJECTIVE 1 - DEVELOPING AND IMPLEMENTING APPROPRIATE CYBER SECURITY RISK MANAGEMENT PRACTICES

The wider use of ICTs creates the risk of increasing numbers of cyber incidents and breaches that can cause severe disruptions in the modern society and major economic damage to businesses. Moreover, those incidents can also undermine the trust of citizens and businesses in the digital society and discourage the use of digital technologies. Weak risk management practices can threaten all partners within value chains and production networks, with consequential effects on national and regional economies. For this reason, ways of raising awareness, especially amongst SMEs, about cyber risks should be explored and the adoption of good consumer practices needs to be encouraged.

Likewise, it is important to support innovative SMEs and high-tech start-ups in the area of cyber security, in order to facilitate their research activities, especially in their early development phases. This also entails them investing in cyber security in order to tackle threats, including those which target trade secrets, related to digitalization.

To this end, we the G7 ICT and Industry Ministers intend to:

1. encourage companies, notably SMEs, at their senior management level to improve awareness and to adopt effective cyber security risk management practices, taking into account comparable risk analysis methodologies;
2. promote cooperation between Governments and companies, particularly SMEs, involving industry associations, academia, tech community associations, security researchers and cyber risk insurance industry, to improve the evidence base on the economic and business impacts of cyber security and data breach incidents;
3. encourage and support consumers to adopt vigilant and proactive practices to safeguard their online identity and to actively use the trust services of their choice.

OBJECTIVE 2 – ENHANCING COOPERATION

Cooperation represents the key factor to strengthen cyber security. There are different levels of cooperation, all equally important: among technical-operational bodies, governments and among governments and enterprises. Each of these types of cooperation should be improved.

Effective and constructive cooperation among G7 countries, national CSIRTs (computer security incident response teams) and between CSIRTs and businesses, can boost chances of preventing and responding to cyber threats through reliable and trusted channels for exchanging actionable information regarding potential and emerging threats. In this environment, the role of national CSIRTs is important as the main focal point, in particular for information sharing at technical and operational level.

Assessing the exposure of enterprises to cybersecurity threats and developing appropriate internal practices can help the enterprises, particularly SMEs, to enhance the security and resilience of their business processes.

Lack of knowledge makes businesses vulnerable to cyber threats and attacks. G7 countries should seek to increase the culture of cyber security and enhance the cybersecurity awareness especially among businesses.

Critical Information Infrastructures are usually handled by the private sector, including SMEs. Sharing information to protect critical information infrastructure from cyber

threats is fundamental for the resilience and security of essential services for citizens and businesses.

Critical Information Infrastructure Protection (CIIP) is part of the digital agenda of many countries as well as international organizations. Some countries have already put in place a national framework and are revising their guidelines on this issue.

For this reason, we the G7 ICT and Industry Ministers intend to explore ways to improve cooperation among the public and private sector, including SMEs, in order to build an environment for the digital economy based on awareness, security and trust.

To this end we intend to:

1. foster constructive cooperation amongst the G7 countries' national CSIRTs and between CSIRTs and businesses of all sizes, in order to exchange information about cyber threats and vulnerabilities;
2. consider common ways to assess the exposure of enterprises to cybersecurity threats and for evaluating the effectiveness of the corresponding cybersecurity measures;
3. encourage the international community through collaboration between business, governments and civil society, to consider a variety of approaches such as security by design, risk management practices, market-relevant conformity assessments and appropriate security evaluation processes, to improve security throughout the value chain and foster greater confidence in the digital economy.
4. conduct awareness campaigns amongst SMEs about cyber security risks and how to manage them;
5. support initiatives to foster a culture of cooperation, notably between governments and businesses, for more effective knowledge of cyber threats and vulnerabilities;
6. promote information sharing through the collaboration of critical information infrastructure operators such as ISAC (Information Sharing and Analysis Centres) or its equivalents.
7. promote global dialogue for co-operation and the sharing of good practice amongst all stakeholders, including cyber security risk management, for economic prosperity.