For Official Use **C(2015)115**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **01-Sep-2015**

English - Or. English

COUNCIL

Council

DRAFT RECOMMENDATION OF THE COUNCIL ON DIGITAL SECURITY RISK MANAGEMENT FOR ECONOMIC AND SOCIAL PROSPERITY

(Note by the Secretary-General)

JT03381164

1. Over ten years, the digital environment has become essential to the functioning of the economy and a key enabler for growth, well-being and inclusiveness. At the same time as they successfully take advantage of Information and Communications Technologies (ICTs) and the Internet to increase their productivity and competitiveness, governments and businesses are exposed to an increasing number of digital security threats, some of which are extremely sophisticated.

2. Routine mainstream media reports about large scale digital security incidents have raised awareness about their potential economic consequences (i.e. the risk). A digital security incident can drastically reduce the benefits an organisation expects from embracing the digital environment. It can cause significant disruption of its business operations, financial losses as well as reputational damage. In some cases, still relatively rare, the incidents can even cause physical destruction of equipment and facilities, with consequences for public safety, and possibly national security (critical infrastructures). Digital security threats can also affect the privacy of organisations' customers, staff and partners. The generalisation of the Internet of Things, which is expected to bring considerable economic and social benefits, will make digital security risk even more pervasive.

3. To fully reap the benefits associated with the digital environment, stakeholders need to firmly depart from approaching digital security risk from a technical perspective in isolation from broader economic and social considerations. It is urgent that they integrate digital security risk management in their economic and social decision making process. Public policy makers also need to ponder the complexity of digital security risk through its multiple dimensions from economic and social prosperity to law enforcement ("cybercrime") to warfare to national security and international security. The proposed draft Recommendation provides guidance in respect of both aspects.

Recommendation

4. Digital security is not an uncharted area for the OECD. In 2002, the Council adopted a *Recommendation Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* [C(2002)131/FINAL] ("Security Guidelines") which replaced the first Security Guidelines, adopted in 1992. Initiated in 2012, the second 5 year review of the 2002 Security Guidelines concluded that they needed to be replaced with a new Recommendation focusing on security risk to economic and social activities supported by the digital environment rather than on the security of the environment itself (information systems and networks). Considering the significantly more important role of ICTs in the economy and the increased level of risk, the review also emphasised the need to develop specific guidance for public policy makers as part of the draft Recommendation.

5. The draft Recommendation of the Council on Digital Security Risk management for Economic and Social Prosperity ("draft Recommendation") set out in Appendix I of this document aims to untangle digital security risk management to help public and private organisations maximise the benefits associated with the digital environment (Section 1). One important objective is to encourage leaders and decision makers (CEOs, Management boards, Executive committees) to own this issue and to integrate digital security risk in their organisation's standard risk management processes. Future work will help better understand how the Recommendation's Principles could be applied by individuals and Small and Medium Enterprises (SMEs) who have much more limited resources than large organisations.

6. The draft Recommendation includes eight principles meant to guide a responsible approach to the use of the digital environment for economic and social prosperity, supported by two key considerations. *First*, it is not possible to eliminate digital security risk other than by forsaking the benefits of digital openness and interconnectedness. Although an entirely "safe and secure" open digital environment cannot be ensured, it is possible to manage the risk, reducing it to an acceptable level in light of the economic and social activities at stake. *Second*, digital security risk management should be an integral part of the decision

to carry out an activity relying in full or in part on the digital environment. Digital security risk management, indeed, relates to the continuity of economic activities relying on the digital environment and not to the functioning of the digital environment itself. The responsibility to manage associated risks should therefore be owned by the leaders, ultimately responsible for achieving economic and social objectives, with the support of the professionals responsible for the technical infrastructure. This is a major change from the 2002 Security Guidelines.

7. The draft Recommendation also includes directions for the development of public policies to foster digital security risk management in the economy and society (Section 2). They relate to what governments often call "national cybersecurity strategies" which should be supported at the highest level of political leadership and result from a co-ordinated intra-governmental and multi-stakeholder approach. This section includes four categories of recommendations calling, for example, on governments to use their market position to encourage risk management, to promote innovation and R&D, the development of skills, as well as mutual international assistance and support.

8. At time of adoption, this Recommendation will be the only international instrument on "cybersecurity" developed from an economic and social perspective. Together with the Privacy Guidelines revised in 2013 [C(2013)79], it will form a robust basis for a better international dialogue on trust in the digital economy. Furthermore, it will support other OECD legal instruments such as the Seoul Declaration for the Future of the Internet Economy (2008) [C(2008)99] and the Recommendation on Internet Policy Making Principles (2011) [C(2011)154], since it promotes an interconnected, open, dynamic and global digital environment conducive to innovation, as well as a multi-stakeholder approach to public policies in this area. It will be an important component of the Ministerial Meeting on the Digital Economy to be held in Cancun, Mexico on 22-23 June 2016.

Companion document

9. The Companion document set out in Appendix II does not form part of the Council Recommendation. It was developed in close connection with the draft Recommendation to facilitate its implementation by providing background information, illustrations and explanations focusing on its first part (the Principles). The Committee on Digital Economy Policy (CDEP) approved the Companion document at its June 2015 meeting. It is provided for information to the Council in support of the draft Recommendation, and, as per para. 7 of the Resolution of the Council on the classification and declassification of information [C(97)64/REV1/FINAL], the Council is responsible for its declassification. The CDEP may in the future update it as necessary in light of new developments or to provide further explanations, and examples.

Participation of non-Members and update of the CDEP's Participation Plan

10. The draft Recommendation is addressed to "Adherents" (i.e. Members and non-Members adhering to it). Adherence by non-Members is particularly relevant because digital security risk takes place in a global and interconnected digital environment in which all stakeholders are interdependent. Thus the larger the number of countries adopting a consistent approach, the greater the benefits to all.

11. As the draft Recommendation is meant to replace the 2002 Security Guidelines, the participation plan [C(2013)67] which currently refers to the latter, needs to be updated. Willingness to adhere to and implement the draft Recommendation would therefore be included in the Participation Plan of the CDEP as a condition to be met by Associates in the Committee.

Process

12. The draft Recommendation and Companion document have been developed on the basis of a one year multistakeholder (i.e. governments, businesses, civil society, Internet technical community) informal consultation in 2013, followed by one year and a half drafting and review period in the Working Party on Security and Privacy in the Digital Economy (SPDE). Eight versions of the draft were discussed including during dedicated drafting meetings. On 25 June 2015, the CDEP approved the draft Recommendation and its transmission to Council for adoption [DSTI/ICCP/REG(2014)2/REV7].

Proposed action

13. In light of the preceding, the Secretary-General invites the Council to adopt the following draft conclusions:

THE COUNCIL

a) noted document C(2015)115;

b) adopted the Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity as set out in Appendix I of document C(2015)115, and agreed to its declassification;

c) agreed to the abrogation of the Recommendation Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security of 25 July 2002 [C(2002)131/FINAL];

d) agreed to replace the reference to the legal instrument mentioned under c) in the Participation Plan of the Committee on Digital Economy Policy [C(2013)67] by a reference to the legal instrument mentioned under b);

e) agreed to the declassification of the Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity, as set out in Appendix II of document C(2015)115;

f) recalled that the participation of non-Members in OECD bodies is governed by the Resolution of the Council on Partnerships in OECD Bodies [C(2012)100/FINAL].

APPENDIX I

DRAFT RECOMMENDATION OF THE COUNCIL ON DIGITAL SECURITY RISK MANAGEMENT FOR ECONOMIC AND SOCIAL PROSPERITY

THE COUNCIL,

HAVING REGARD to the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, articles 1 b), 1 c), 3 a), 3 b) and 5 b) thereof;

HAVING REGARD to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines") [C(80)58/FINAL as amended]; the Recommendation of the Council concerning Guidelines for Cryptography Policy [C(97)62/FINAL]; the Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]; the Declaration for the Future of the Internet Economy (The Seoul Declaration) [C(2008)99]; the Recommendation of the Council on Principles for Internet Policy Making [C(2011)154]; the Recommendation of the Council on Regulatory Policy and Governance [C(2012)37]; the Recommendation of the Council on Digital Government Strategies [C(2014)88]; and the Recommendation of the Council on the Governance of Critical Risks [C/MIN(2014)8/FINAL];

HAVING REGARD to the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security [C(2002)131/FINAL], which this Recommendation replaces;

RECOGNISING that the digital environment, including the Internet, is essential to the functioning of our economies and societies and stimulates growth, innovation, well-being and inclusiveness;

RECOGNISING that the benefits from the digital environment span across all sectors of the economy and all aspects of social progress; that these benefits stem from the global, open, interconnected and dynamic nature of information and communication technologies and infrastructure, and in particular the Internet;

RECOGNISING that the use, management and development of the digital environment are subject to uncertainties which are dynamic in nature;

RECOGNISING that digital security risk management is a flexible and agile approach to address these uncertainties and to fully achieve the expected social and economic benefits, to provide essential services and operate critical infrastructures, to preserve human rights and fundamental values, and to protect individuals from digital security threats ;

EMPHASISING that digital security risk management provides a robust foundation to implement the "Security Safeguards Principle" in the OECD Privacy Guidelines and, more generally, that this Recommendation and the OECD Privacy Guidelines mutually reinforce each other;

MINDFUL that governments, public and private organisations, as well as individuals share responsibility, based on their roles and the context, for managing digital security risk and for protecting the digital environment; and that co-operation is essential at domestic, regional and international levels.

On the proposal of the Committee on Digital Economy Policy:

I. RECOMMENDS that Members and non-Members adhering to this Recommendation (hereafter the "Adherents"):

1. Implement the principles set out in Section 1 (hereafter the "Principles") at all levels of government and in public organisations;

2. Adopt a national strategy for the management of digital security risk as set out in Section 2;

II. CALLS ON the highest level of leadership in government and in public and private organisations to adopt a digital security risk management approach to build trust and take advantage of the open digital environment for economic and social prosperity;

III. ENCOURAGES private organisations to adopt the Principles in their approach to digital security risk management;

IV. ENCOURAGES all stakeholders to implement the Principles in their decision making processes, based on their roles, ability to act and the context;

V. CALLS ON governments and public and private organisations to work together to empower individuals and small and medium enterprises to collaboratively manage digital security risk;

VI. AGREES that the Principles are complementary and should be taken as a whole, and that they are meant to be consistent with risk management processes, best practices, methodologies, and standards;

VII. AGREES further that, for the purposes of this Recommendation:

1. Risk is the effect of uncertainties on objectives. "Digital security risk" is the expression used to describe a category of risk related to the use, development and management of the digital environment in the course of any activity. This risk can result from the combination of threats and vulnerabilities in the digital environment. It can undermine the achievement of economic and social objectives by disrupting the confidentiality, integrity and availability of the activities and/or the environment. Digital security risk is dynamic in nature. It includes aspects related to the digital and physical environments, the people involved in the activity and the organisational processes supporting it.

2. "Digital security risk management" is the set of coordinated actions taken within an organisation and/or among organisations, to address digital security risk while maximising opportunities. It is an integral part of decision making and of an overall framework to manage risk to economic and social activities. It relies on a holistic, systematic and flexible set of cyclical processes that is as transparent and as explicit as possible. This set of processes helps to ensure that digital security risk management measures ("security measures") are appropriate to and commensurate with the risk and economic and social objectives at stake.

3. "Stakeholders" are the governments, public and private organisations, and the individuals, who rely on the digital environment for all or part of their economic and social activities. They can

cumulate different roles. “Leaders and decision makers” are those stakeholders at the highest level of leadership in government and in public and private organisations.

SECTION 1. PRINCIPLES

General Principles

1. *Awareness, skills and empowerment*

All stakeholders should understand digital security risk and how to manage it.

They should be aware that digital security risk can affect the achievement of their economic and social objectives and that their management of digital security risk can affect others. They should be empowered with the education and skills necessary to understand this risk to help manage it, and to evaluate the potential impact of their digital security risk management decisions on their activities and the overall digital environment.

2. *Responsibility*

All stakeholders should take responsibility for the management of digital security risk.

They should act responsibly and be accountable, based on their roles, the context and their ability to act, for the management of digital security risk and for taking into account the potential impact of their decisions on others. They should recognise that a certain level of digital security risk has to be accepted to achieve economic and social objectives.

3. *Human rights and fundamental values*

All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.

Digital security risk management should be implemented in a manner that is consistent with human rights and fundamental values recognised by democratic societies, including the freedom of expression, the free flow of information, the confidentiality of information and communication, the protection of privacy and personal data, openness and fair process. Digital security risk management should be based on ethical conduct which respects and recognises the legitimate interests of others and of the society as a whole. Organisations should have a general policy of transparency about their practices and procedures to manage digital security risk.

4. *Co-operation*

All stakeholders should co-operate, including across borders.

Global interconnectedness creates interdependencies between stakeholders and calls for their co-operation on digital security risk management. Co-operation should include all stakeholders. It should take place within governments, public and private organisations, as well as amongst them and with individuals. Co-operation should also extend across borders at regional and international levels.

Operational Principles

5. *Risk assessment and treatment cycle*

Leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment.

Digital security risk assessment should be carried out as an ongoing systematic and cyclical process. It should evaluate the potential consequences of threats combined with vulnerabilities on the economic and social activities at stake, and inform the decision making process for treating the risk. The

treatment of the risk should aim to reduce the risk to an acceptable level relative to the economic and social benefits expected from those activities while taking into account the potential impact on the legitimate interests of others. Risk treatment includes various options: accepting the risk, reducing it, transferring it, avoiding it or a combination of those.

6. ***Security measures***

Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.

Digital security risk assessment should guide the selection, operation and improvement of security measures to reduce the digital security risk to the acceptable level determined in the risk assessment and treatment. Security measures should be appropriate to and commensurate with the risk and their selection should take into account their potential negative and positive impact on the economic and social activities they aim to protect, on human rights and fundamental values, and on the legitimate interests of others. All types of measures should be considered, whether they are physical, digital, or related to people, processes or technologies involved in the activities. Organisations should seek out and appropriately address vulnerabilities as soon as possible.

7. ***Innovation***

Leaders and decision makers should ensure that innovation is considered.

Innovation should be considered as integral to reducing digital security risk to the acceptable level determined in the risk assessment and treatment. It should be fostered both in the design and operation of the economic and social activities relying on the digital environment as well as in the design and development of security measures.

8. ***Preparedness and continuity***

Leaders and decision makers should ensure that a preparedness and continuity plan is adopted.

Based on digital security risk assessment, a preparedness and continuity plan should be adopted to reduce the adverse effects of security incidents, and support the continuity and resilience of economic and social activities. The plan should identify measures to prevent, detect, respond and recover from digital security incidents. It should provide mechanisms to ascribe clear levels of escalation based on the magnitude and severity of the effects of digital security incidents, as well as their potential to extend to others in the digital environment. Appropriate notification procedures should be considered as part of the implementation of the plan.

SECTION 2. NATIONAL STRATEGIES

A. National strategies for the management of digital security risk should be consistent with the Principles and create the conditions for all stakeholders to manage digital security risk to economic and social activities and to foster trust and confidence in the digital environment. These strategies should:

1. Be supported at the highest level of government and articulate a clear and whole-of-government approach that is flexible, technology-neutral and coherent with other strategies fostering economic and social prosperity;

2. Clearly state that they aim to take advantage of the open digital environment for economic and social prosperity by reducing the overall level of digital security risk within and across borders without unnecessarily restricting the flow of technologies, communications and data;

that they also aim to ensure the provision of essential services and the operation of critical infrastructures, to protect individuals from digital security threats while taking into account the need to safeguard national and international security, and to preserve human rights and fundamental values;

3. Be directed at all stakeholders, tailored as appropriate to small and medium enterprises and to individuals, and articulate stakeholders' responsibility and accountability according to their roles, ability to act and the context in which they operate;

4. Result from a coordinated intra-governmental approach and an open and transparent process involving all stakeholders, be regularly reviewed and improved based on experience and best practices, using internationally comparable metrics where available.

B. National strategies should include measures whereby governments:

1. ***Lead by example****, notably by:*

i) Adopting a comprehensive framework to manage digital security risk to the government's own activities. The framework and implementing policies should be transparent in order to foster trust and confidence in government activities and behaviour, including with respect to responsible disclosure of the digital security vulnerabilities they have identified, and related mitigation measures;

ii) Establishing co-ordination mechanisms among all relevant governmental actors to ensure that their management of digital security risk is compatible and enhances economic and social prosperity;

iii) Ensuring the establishment of one or more Computer Security Incident Response Team (CSIRT), also known as Computer Emergency Response Team (CERT), at national level and, where appropriate, encourage the emergence of public and private CSIRTs working collaboratively, including across borders;

iv) Using their market position to foster digital security risk management across the economy and society, including through public procurement policies, and the recruitment of professionals with appropriate risk management qualification;

v) Encouraging the use of international standards and best practices on digital security risk management, and promoting their development and review through open, transparent and multi-stakeholder processes;

vi) Adopting innovative security techniques to manage digital security risk in order to assure that information is appropriately protected at rest as well as in transit, and taking into account the benefits of appropriate limitations on data collection and retention;

vii) Coordinating and promoting public research and development on digital security risk management with a view to fostering innovation;

viii) Supporting the development of a skilled workforce that can manage digital security risk, in particular by addressing digital security risk management in broader skills strategies. This could include fostering the development of in-service risk management training and certification and supporting the development of digital skills across the population through national education programmes, notably in higher education;

ix) Adopting and implementing a comprehensive framework to help mitigate cybercrime, drawing on existing international instruments**;**

x) Allocating sufficient resources to effectively implement the strategy.

2. ***Strengthen international co-operation and mutual assistance****, notably by:*

i) Participating in relevant regional and international fora, and establishing bilateral and multilateral relationships to share experience and best practices; and promoting an approach to national digital security risk management that does not increase the risk to other countries;

ii) Providing, on a voluntary basis as appropriate, assistance and support to other countries, and establishing national points of contacts for addressing cross-border requests related to digital security risk management issues in a timely manner;

iii) Working to improve responses to domestic and cross-border threats, including through CSIRTs co-operation, coordinated exercises and other tools for collaboration.

3. ***Engage with other stakeholders****, notably by:*

i) Exploring how governments and other stakeholders can help each other to better manage digital security risk to their activities;

ii) Identifying and addressing potential negative impacts that government policies may have on other stakeholders' activities or national economic and social prosperity;

iii) Establishing practices and procedures for digital security risk management, made known to the public;

iv) Encouraging the responsible discovery, reporting and/or correction of digital security vulnerabilities by all stakeholders;

v) Raising the level of awareness, skills and empowerment across society to manage digital security risk through technology-neutral initiatives tailored to the specific needs of the different categories of stakeholders.

4. ***Create the conditions for all stakeholders to collaborate in the management of digital security risk****, notably by:*

i) Fostering active participation from relevant stakeholders in mutually trusted initiatives and partnerships whether private or public-private, formal or informal, at domestic, regional and international levels to:

– Share knowledge, skills and successful experience and practices in relation to digital security risk management at policy and operational levels;

– Exchange information related to digital security risk management;

– Anticipate and plan for future challenges and opportunities.

ii) Foster co-ordination among stakeholders to improve identification and remediation of vulnerabilities and threats, as well as mitigation of digital security risk;

iii) Encouraging all stakeholders to work together to help protect individuals and small and medium enterprises from digital security threats and increase their ability to manage digital security risk to their economic and social activities;

iv) Providing incentives, as appropriate, to stakeholders to manage digital security risk and increase market transparency and efficiency;

v) Encouraging innovation in digital security risk management as well as in the development of tools that individuals and organisations can use to protect their activities in the digital environment;

vi) Encouraging the development of internationally comparable risk metrics based on common measurement methodologies, standards and best practices, as appropriate, to improve effectiveness, efficiency and transparency in the management of digital security risk.

VIII. RECOMMENDS that Adherents co-operate in the implementation of this Recommendation, promote and disseminate it throughout the public and private sectors, to non-Adherents and international fora;

X. INVITES non-Members to adhere to this Recommendation;

XI. INSTRUCTS the Committee on Digital Economy Policy to review the implementation of this Recommendation and to report to Council within three years of its adoption and thereafter as appropriate.

APPENDIX II

COMPANION DOCUMENT TO THE RECOMMENDATION OF THE COUNCIL ON DIGITAL SECURITY RISK MANAGEMENT FOR ECONOMIC AND SOCIAL PROSPERITY

NOTE BY THE SECRETARIAT

This document is explanatory and illustrative in nature and does not form part of the *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*.

It was developed by the OECD Working Party on Security and Privacy in the Digital Economy (SPDE), approved by its parent body, the Committee on Digital Economy Policy (CDEP) on 25 June 2015 and declassified by the OECD Council on [DATE].

TABLE OF CONTENTS

INTRODUCTION

1. Over the last ten years, Information and Communications Technologies (ICTs), including the Internet, have become essential to the functioning of the economy as well as a key driver for development in all sectors. Governments, public and private organisations as well as individuals have become dependent on the digital environment for their core activities. However, they are facing a growing number of uncertainties related to the use of the digital environment. Digital security threats and incidents have increased, leading to significant financial, privacy, and reputational consequences, and in some cases even to physical damages. Although stakeholders are increasingly aware of the challenges raised by digital security risk, they often approach it only from the technical perspective, and in a manner isolated from economic and social decision making. It has become urgent to explain that digital security risk management should be, first and foremost, integral to economic and social decision making in order to enable stakeholders to fully benefit from the opportunities offered by the digital environment.

2. Digital security issues are often captured through the convenient catch-all term "cybersecurity", covering all digital security dimensions from technology, to economic and social, legal, law enforcement, human rights, national security, warfare, international stability, intelligence, and other aspects. The widespread use of this term often masks the broad and complex nature of the subject matter. Digital security can be approached from at least four different perspectives each stemming from a different culture and background, recognised practices, and objectives:

- Technology, i.e. focusing on the functioning of the digital environment (often called "information security", "computer security", or "network security" by experts);
- Law enforcement and, more generally, legal aspects (e.g. cybercrime);
- National and international security, including aspects such as the role of ICTs with respect to intelligence, conflicts prevention, warfare, etc.
- Economic and social prosperity, encompassing wealth creation, innovation, growth, competitiveness and employment across all economic sectors[1], as well as aspects such as individual liberties, health[2], education[3], culture, democratic participation, science, leisure, and other dimensions of well-being in which the digital environment is driving progress;

3. Consistent with its mandate to promote "Better policies for better lives", the OECD approaches digital security risk from the economic and social perspective.

4. In 2015, the OECD Council[4] adopted the *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity* (the "Recommendation") as part of a broader set of Recommendations, guidance and analytical work on digital economy policy.[5] Resulting from over two years of work, the Recommendation builds on three decades of OECD experience in developing policies and instruments for innovation and trust in the digital economy, starting with the 1980 *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ("Privacy Guidelines", amended in 2013) and including legal instruments related to cryptography policy, electronic authentication, and the protection of critical information infrastructures,

among others. The Recommendation replaces the 2002 *Recommendation of the Council Concerning Guidelines for the Security of Systems and Networks: Towards a Culture of Security*, ("Security Guidelines") which itself replaced the 1992 *Recommendation of the Council Concerning Guidelines for the Security of Information Systems* ("first Security Guidelines"). It is therefore the third milestone in a maturation process reflecting the evolution of the digital economy and in particular its essential role for the successful functioning and development of all economic sectors and social life.

5. All Recommendations are non-legally binding Acts of the Organisation, but practice accords them great moral force as representing the political will of Member countries. There is an expectation that Members and non-Members having adhered to them (the "Adherents") will do their utmost to fully implement them.[6] This Recommendation was agreed upon by consensus and informed by a multistakeholder process involving government policy makers, business and industry, civil society, and the technical community.[7] Governments beyond OECD membership are encouraged to use it to inform the development of their national strategies, whether they chose to formally adhere to the Recommendation or not. In addition, all public and private organisations are encouraged to take into account its Principles in their own risk management frameworks. Other international and regional organisations are welcome, and even encouraged, to reflect this Recommendation in their own work and activities.[8]

6. The Recommendation recognises that the various dimensions mentioned above (economic, social, technical, law enforcement, national security and international security) are as interrelated in the digital environment as they are outside of it. Governments should therefore strive for a whole-of-government approach to the different dimensions of digital security risk, aspiring for coherence, complementarity and mutual reinforcement.

7. In this respect, the Recommendation calls on governments to adopt a national strategy for the management of digital security risk (I.2) supported at the highest level of government (Section 2. A. 1) to ensure that competing policy objectives are appropriately balanced. It is expected that the implementation of the Recommendation will foster co-operation among experts addressing the various perspectives of digital security issues, at the domestic, regional and international levels.

8. It is important to highlight that the Recommendation, and more generally OECD work in this area, is part of an international dialogue involving several organisations, with complementary streams of work reflecting their specific mandate. For example, the Council of Europe addresses issues related to cybercrime (e.g. 2001 Budapest Convention on Cybercrime)[9]; Interpol facilitates operational law enforcement co-operation[10]; the United Nations[11] and the Organization for Security and Cooperation in Europe (OSCE)[12] discuss States' behavior in the digital environment and confidence building measures to preserve international stability; technical standards are being developed in a variety of settings, such as the International Organization for Standardization (ISO), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS), etc. Regional organisations such as the Asia-Pacific Economic Cooperation (APEC)[13] also play a key role to foster implementation of best practices and guidelines.

9. The Recommendation starts with a preamble ("Having regards", "Recognising", etc.), followed by numbered recommendations from the Council (thereafter "the OECD") to governments and other stakeholders (e.g. "I. Recommends…", "II. Calls on…", etc.), as well as information regarding the Principles ("VI. Agrees…") and clarifications about the terminology ("VII Agrees further…"). In this part, the OECD calls on the highest level of leadership in government and in public and private organisations to adopt an approach to digital security risk management that builds trust and takes advantage of the open digital environment for economic and social prosperity (point II).

10. Section 1 provides a coherent framework of eight interrelated, interdependent and complementary high-level principles on digital security risk management (thereafter "the Principles"). The OECD recommends that Adherents implement these Principles at all levels of government[14] and in public organisations (point I.1). It also encourages private organisations, including businesses and nonprofit, to adopt these Principles in their approach to digital security risk management (point III), and to implement them in their decision making processes based on the their roles, ability to act and the context[15] (point IV).

11. Thus the Principles can be used directly to guide public or private organisations in the development of their corporate or organisational risk management policy, or indirectly, to inspire the development of a national strategy and related public policies. Precisely, the Recommendation recommends that Adherents adopt a national strategy for the management of digital security risk, following the guidance provided in its Section 2, which, albeit presented with a different structure, was developed on the basis of the Principles.

12. In general, the Recommendation addresses primarily the highest level of leadership ("leaders and decision makers") who is best placed to steer the adoption of, in organisations, an appropriate digital security risk management governance framework, and, in governments, a national strategy conducive to economic and social prosperity.

13. Since the early stages of the Recommendation's drafting process, OECD delegations have recognised the complexity of the subject matter and the need to facilitate the Recommendation's implementation by developing a separate document containing background information and explanations. They also agreed that this "Companion document" would need to be short and address only the most fundamental aspects of digital security risk management, and therefore focus only on Section 1 of the Recommendation. Future work could address in more detail some of the issues identified in this Companion document as well as the need for public policy guidance reflected in Section 2 of the Recommendation. The Annex provides a list of possible areas for future work identified in this Companion document as well as during the course of the consultation and drafting process.

14. After a brief description of the context, this document discusses the key concepts in the Recommendation, comments on the applicability of the Principles to stakeholders, and finally provides an explanation of each of the eight Principles.

CONTEXT

15. Many leaders and decision makers in public and private organisations are realising that in addition to being a driver for innovation, productivity and growth, the digital environment also introduces uncertainties that can jeopardise economic and social prosperity. Digital security incidents can have far reaching economic consequences for organisations, for example in terms of disruption of operations (e.g. through denial of service or sabotage), direct financial loss, lawsuits, reputational damage, loss of competitiveness (e.g. in case of theft of trade secrets), as well as loss of trust among their customers, employees, shareholders and partners. Although cases are still exceptional, one should also consider the possibility that digital security incidents can cause physical damages including loss of human life, considering the increasing ICT reliance of industrial facilities, transportation systems and hospitals.

16. Governments are facing the same potential consequences from security incidents as other organisations. As developers of public policy, they are also concerned by consequences of incidents at a macro level, encompassing aspects that extend beyond the economic and social sphere to national and international security, as noted above.

17. Finally, individuals are increasingly aware that there can be a downside to the many benefits they derive from the use of the digital environment. When their personal data is publicly disclosed or falls into the hands of unauthorised persons, individuals face privacy breaches with potential physical, material and moral damage.[16] They can be victims of financial fraud in relation to identity theft when their personal data or digital credentials are stolen from their own devices, from compromised companies, or governments' information systems.

18. The increased volume of incidents and their increased sophistication result from many factors. One of them is the migration of criminal activities online which has been driving the professionalisation of attacks and increasing the overall digital security threat level. From the occasional isolated robber to well-organised transnational groups, criminals have been demonstrating considerable technical innovation skills to commit financial, information and identity theft and blackmail individuals, businesses and governments. Other factors include terrorists and their supporters who have also extended their actions to the digital environment, multiplying attacks of Internet sites in conjunction with physical attacks or in addition to them. Although few cases have been extensively documented, industrial digital espionage has been mentioned as being on the rise. So-called "hacktivists" routinely attack selected targets to increase the visibility of their political cause. Finally, many governments are carrying out intelligence and offensive operations in what they often call the "cyberspace". Long gone are the days when the main source of security-related digital uncertainty consisted of teenagers launching random attacks using readymade tools available online ("script kiddies").

19. The professionalisation of threat sources has led to increased sophistication of offensive technical tools, some of which are automated and deployed on a large scale for maximum impact, while others are carefully tailored to specific valuable targets and to evade detection and attribution. An underground cybercrime economy has emerged. So-called "zero-day exploits", i.e. malicious code that can pass most protection software, are available for purchase on digital marketplaces. They are used to stealthily penetrate information systems, monitor them and then extract confidential data such as trade or political secrets over extensive periods of time (called Advanced Persistent Threat, "APT").[17] Botnets comprising thousands to millions[18] of infected computers and devices can be rented to perform denial of service

attacks in order to blackmail their owner or to express discontent. Social engineering techniques are also very common, for example through emails that look legitimate but enable the attacker to steal credentials or penetrate the user's system ("phishing"). Box 1 provides examples of large scale incidents which have raised awareness about the scope and scale of this challenge.

Box 1. 2007-2014: Examples of large-scale incidents

Although robust and internationally comparable quantitative metrics are difficult to develop in this area (OECD, 2012c), empirical evidence shows that digital security incidents are multiplying and that they concern everyone: public and private organisations, individuals and governments. It includes the following examples.

In 2007, massive "cyberattacks" against Estonia affected the parliament, ministries, banks, newspapers and broadcasters.

In 2010, the Stuxnet worm physically destroyed hundreds of centrifuges at a nuclear enrichment plant in Iran. In 2011, intruders compromised the Sony PlayStation Network, disclosing personal data from over 77 million accounts and costing the company, officially, USD 171 million and perhaps up to USD 250 million according to some estimates.(Gaudiosi, 2014)

In 2012, it took over two weeks for the oil company Saudi Aramco's to recover from the erasure of over 30 000 hard drives connected to its internal network by digital intruders.

In 2013, a massive denial of service (DoS) attack was carried out against the anti-spam organisation Spamhaus, peaking at an unprecedented 300 Gigabits per second (Gbs), six times the average DoS attack and three times the largest denial of service attack ever detected (Leyden, 2013). The same year, the US retail company Target was hit during the Christmas sales season by a sophisticated attack involving point of sale devices through which 40 million credit and debit card numbers and over 110 million customer records were stolen, costing the company from USD 148 million to over a billion, depending on estimates. A few weeks later, its CEO resigned (O'Connor , 2014).

In 2014, the US firm Home Depot also faced the theft of 56 million credit and debit card information. In, Korea, a man stole personal data on 104 million credit cards issued by three major banks, affecting 20 million individuals (40% of the country's population). Dozens of senior executives lost their jobs as a result (Choe, 2014. Kim, 2014). Later in the year, account data associated with 76 million US households and seven million small businesses was compromised at US bank JP Morgan Chase, after which its CEO stressed that the company's digital security budget would likely double from USD 250 million to 500 million (Kitten, 2014). The same year, an in-depth intrusion in Sony Pictures Entertainment's internal network led to public disclosure of internal emails, personal data of company employees and partners as well as movies that were not yet on the market; a large scale cyber espionage operation targeting primarily European and US companies in the pharmaceutical and perhaps energy sectors was detected (Dragonfly) (Peters, 2014) . Finally, an intrusion in the network of a steel facility in Germany led to "massive physical damage" (Lee, Assante, Conway, 2014).

20. As of 2009, digital security challenges progressively became a national public policy priority in OECD countries. A number of governments began to adopt "national cybersecurity strategies" supported at the highest political level. These strategies promoted a holistic public policy approach and established new coordination mechanisms both within the government and with non-governmental stakeholders.[19]

21. Public and private sector organisations are progressively[20] recognising the scale of the challenge and adjusting their practices. In particular, an increasing number of top senior executives in large firms understand that a purely technical approach is insufficient to manage digital security risk. However, many public and private organisations, and in particular Small and Medium Enterprises (SMEs), are not yet ready to manage digital security risk from an economic perspective and still consider this issue as mainly technical. Finally, the increasing number of massive data breaches exposing personal data and leading in some cases to financial fraud and identity theft raises concerns among individuals[21] who are often left on their own, without the means, knowledge and skills to effectively manage this risk.

Box 2. From "security of information systems" to "digital security risk management" (2002-2015)

The 2015 Recommendation represents both a continuation of and a major change from the 2002 Security Guidelines.

Both Recommendations start from the same analysis: *i)* the global, interconnected, open and dynamic nature of the digital environment is essential to drive economic and social prosperity, *ii)* it is impossible to create a "safe and secure" digital environment where risk is entirely avoided other than by eliminating digital openness, interconnectedness and dynamism, and giving up the economic and social benefits these properties can unleash. Thus both Recommendations confirm the abandonment of the pre-Internet static and rigid "perimeter security" in favor of a cyclical and agile risk-based approach, whereby risk is managed. That is, it is reduced to an acceptable level according to the context and objectives at stake.

The major change is that the focus of the Principles has been reoriented from the "security of information systems and networks" to the security risk to the economic and social activities relying on the digital environment. The Recommendation assumes that leaders and decision makers ultimately responsible for carrying out an activity are the best placed to set the acceptable level of risk to this activity and ensure that the digital security measures are appropriate to and commensurate with the risk, and do not undermine the activity they aim to protect. Nevertheless, the Recommendation underlines the need for co-operation with experts in charge of designing and maintaining the digital environment (i.e. ICT professionals) who are likely to better understand the digital security risk factors and related possible security measures.

Accordingly, the risk-related language has been clarified. It was noted during the drafting process that the dictionary definition of "security" – "the state of being free from harm or danger"– suggests a binary and static objective inherently in contradiction with the concept of risk management. For some audiences, "security" relates to "national security", an area often associated, rightly or wrongly, to a culture where "security" is paramount, above any other consideration. Thus, in contrast with the 2002 Security Guidelines, the Recommendation uses "security" as an adjective characterising the risk, risk factors, and risk management approach rather than as a noun pointing to a standalone objective. Likewise, the Recommendation does not use the term "cybersecurity" nor the prefix "cyber" (e.g. as in "cyberspace") which can create confusion as they are understood differently by different audiences. Furthermore, they can convey the false impression that digital security risk is somehow fundamentally different from other categories of risk.

KEY CONCEPTS

22. This section introduces the key concepts used in the Recommendation.

Stakeholders and their roles

23. For the purpose of the Recommendation, "stakeholders" are considered as "the governments, public and private organisations, and the individuals, who rely on the digital environment for all or part of their economic and social activities. They can cumulate different roles." (cf. point VII, 3)

24. This term aims to capture all entities which, to varying degrees, rely on the digital environment to carry out economic and/or social activities in order to accomplish their mission. This sociological rather than legal concept implies a direct and/or indirect usage of the digital environment. The term "government" covers all governmental bodies at all levels (e.g. central/federal, international/regional/national/provincial/local, etc.). "Public sector organisations" include all other entities subject to public or administrative law, such as other administrations funded through taxation (e.g. hospitals, schools, public libraries, etc.) and publicly owned corporations. Private organisations are subject to private law and include businesses as well as non-profit organisations.

25. All stakeholders can have different roles and cumulate them. For example, an individual can be a citizen, consumer, parent, student, worker, etc. depending on the activity being considered. Most organisations are users of the digital environment. As part of their core activities, some are also involved in its operation, management or design (e.g. a software or hardware maker, a telecommunications operator or an Internet service provider). Organisations beyond a certain size often include an Information Technology (IT) department responsible for providing the digital infrastructure that supports the organisation's activities. Some individuals are also involved in the operation of the digital environment without being part of an organisation, such as an app or software developer. Governments can also cumulate different roles: they are users of the digital environment and heavily rely on it (e.g. for e-government as well as to operate most other governmental functions, such as for paying civil servants), and they also adopt public policies to foster economic and social prosperity, including with respect to the digital environment.

Digital security risk

> Extract from the Recommendation (point VII.1):
> "Risk is the effect of uncertainties on objectives. "Digital security risk" is the expression used to describe a category of risk related to the use, development and management of the digital environment in the course of any activity. This risk can result from the combination of threats and vulnerabilities in the digital environment. They can undermine the achievement of economic and social objectives by disrupting the confidentiality, integrity and availability of the activities and/or the environment. Digital security risk is dynamic in nature. It includes aspects related to the digital and physical environments, the people involved in the activity and the organisational processes supporting it."

26. The activities stakeholders undertake in pursuance of their objectives are subject to factors that can have consequences on their likelihood of success. Uncertainty is part of human life: our knowledge and

understanding of such factors and how they could impact our objectives is limited. "Risk" is the effect, or the consequences, of uncertainty on the objectives pursued by stakeholders, that is, the deviation that reality can impose over what they anticipate. This approach of risk is based on ISO/IEC 31000:2009, ISO/IEC 27000 series and ISO Guide 73 (see Box 3). Risk is often expressed in terms of likelihood and impact, and risk levels are typically represented on a X-Y axis, which helps consider the various combinations of these two dimensions.

27. Digital security risk, as defined for the purpose of the Recommendation (see Box 3), is one among many other categories of risk faced by stakeholders. It:

- *Is related to "digital uncertainty", but not only.* Wherever there is some reliance on ICT, there is also some corresponding degree of uncertainty related to the use of the digital environment ("digital uncertainty"). However, digital security risk does not only relate to "zeros and ones": reliance on the digital environment requires software, hardware, and direct or indirect human intervention or interaction, all aspects which can be subject to threats, vulnerabilities and incidents. For example, the availability of a service or production line can be disrupted by a natural disaster affecting the provision of energy to a data centre or cutting aerial cables; and trade secrets can be stolen by criminals using social engineering techniques that manipulate and deceive people into performing actions that enable illegitimate access to information systems. Thus threats, vulnerabilities and incidents can have a digital as well as a physical or human dimension.

- *Is economic and social.* The effects or consequences of digital uncertainty are economic and social and can affect tangible or intangible assets. The risk should therefore be formulated in economic and social terms: financial loss, loss of competitiveness, loss of opportunity, damage to reputation, image or trust, etc. Depending on the context, there may be other effects – i.e. categories of risk –, beyond the scope of the Recommendation, that should however be addressed. For example, organisations may consider purely technical (i.e. ICT) consequences, and governments may address consequences related to national and international security.

- *Affects availability, integrity and confidentiality* (i.e. "security"). Events that can generate effects are the disruption of availability, integrity and confidentiality of the activities or of the digital environment in which they are carried out or on which they directly or indirectly rely. This so-called "AIC triad" represents classic security properties or attributes that help delineate the scope of digital security risk management as a specific field of expertise. Thus, for example, digital security risk does not cover uncertainties related to the violation of intellectual property rights or the dissemination of inappropriate information (*i.e.* content) in the digital environment.[22]

- *Has a negative effect.* In everyday language, "risk" generally captures only the detrimental effects of uncertainty and, accordingly, the Recommendation focuses on uncertainties that can undermine the achievement of economic and social objectives. It approaches digital security risk management as a means to *protect value* to best achieve economic and social objectives. However, uncertainties can also have positive effects and benefit an activity. The beneficial effect of uncertainties is often called "opportunity" rather than risk. The relationship between risk and opportunity is important as digital security risk management could also be used to *create value* by systematically detecting and taking advantage of uncertainties to drive innovation. This is further detailed below (Innovation Principle).

Risk factors: threats, vulnerabilities and incidents

28. Risk can result from events whereby threats combined with vulnerabilities generate economic consequences. Events that can change the expected course of activities and impact objectives are often called *incidents*. Both threats and vulnerabilities are necessary to create consequences for the activity. Threats without vulnerabilities, or vulnerabilities without threats do not increase the risk.

29. Everyday language uses the term "risk" in a loose way. For example, it can be used to mean threat, vulnerability, incident, likelihood, chance and danger.[23] Risk management, however, requires a clear distinction between causes and their consequences and addresses the former (threats, vulnerabilities and incidents) in order to manage the latter (risk). To underline this difference, threats, vulnerabilities and incidents are called "risk factors" in this document, i.e. causes of or contributors to risk.

30. Threats are generally external to the activity while vulnerabilities are weaknesses usually within the activity. As a result, stakeholders often have limited ability to influence threats whereas they can usually act more directly on vulnerabilities. In some cases, both the threat and vulnerability come from within the activity, such as in the case of a disgruntled employee using his/her privileges to perform unauthorised actions leading to detrimental consequences for the employer.

Box 3. About definitions, terminology and standards

The terms and definitions used in the Recommendation should not be interpreted in a prescriptive or rigid manner or as favouring particular risk-related terminology or terms of art over others. They have been chosen to support high-level policy guidance and to accommodate an audience of leaders and decision makers from different countries, cultures, legal regimes, as well as economic, social and political situations, within and beyond OECD membership.

To the extent possible, the Recommendation's risk-related terminology is based on ISO/IEC international standards and guides on risk management and in particular ISO/IEC 31000:2009 and ISO Guide 73 – also reflected in ISO/IEC 27000 series – while recognising that there are many other risk-related standards with sometimes different terminologies.[24] In many cases, terms and definitions have been tailored to the Recommendation's target audiences, objectives and scope. As noted in the Recommendation, the Principles are meant to be consistent with existing risk management processes, best practices, methodologies and standards. It is expected that the Recommendation will help bridge leaders and high-level decision makers with experts in charge of implementing these standards, for the benefit of economic and social prosperity.

Risk management is a complex area which cuts across many different sectors, from health to finance, engineering, insurance, and industrial processes, which all have their own risk culture, terminology and standards. The Recommendation does not purport to present a definitive and overarching understanding of risk and risk management. Risk is an old concept which has been continually evolving throughout history and is still subject to change. There is no universally agreed definition of risk or risk terminology: a researcher recently analysed no less than 27 definitions of risk grouped in nine categories, while recognising that there are probably more. [25]

31. There are many categories and taxonomies of threats, vulnerabilities and incidents. For example, a threat can be intentional (i.e. an attack, such as criminals trying to steal something) or unintentional (i.e. resulting from an accident such as road construction work breaking a fiber optic cable). An incident can also result from human actions such as unintentional errors or individuals manipulated by social engineering techniques (e.g. phishing), as well as from natural events such as storms, floods or earthquakes. The degree of sophistication of intentional threats can range from very simple to extremely complex, as illustrated by sources of intentional threats ranging from young teenagers to State-sponsored groups. Finally, the duration of incidents can vary from extremely short, such as a sudden denial of service attack degrading the communication channel with customers at the highest sales period of the year, to

extremely long (i.e. multi-year), such as in the case of a stealthy intrusion in an information system to eliminate a company from the marketplace by stealing its trade secrets.

32. The dynamic nature of digital security risk results from the ever changing character of all its components: the economic and social activities, the risk factors, and the digital environment.

Digital security risk management

Extract from the Recommendation (point VII.2): ""Digital security risk management" is the set of coordinated actions taken within an organisation and/or among organisations, to address digital security risk while maximising opportunities. It is an integral part of decision making and of an overall framework to manage risk to economic and social activities. It relies on a holistic, systematic and flexible set of cyclical processes that is as transparent and as explicit as possible. This set of processes helps to ensure that digital security risk management measures ("security measures") are appropriate to and commensurate with the risk and economic and social objectives at stake."

33. Digital security risk cannot be eliminated (as noted in Box 2) but it can be managed to promote and protect economic and social activities. Thus digital security risk management aims to foster the achievement of economic and social objectives. In particular, it:

- *Is strategic to economic and social decision making.* Risk management is the process whereby decision makers take into account, in the design and operation of their activities, the factors that can influence the achievement of their objectives. Insofar as their economic and social activities rely, directly or indirectly, on the digital environment, digital security risk management should be integral to their decision making process and considered together with their strategies to maximise opportunities (see Innovation Principle below). Leaders should view digital security risk management as an economic and social rather than purely technical challenge. However, they should co-operate with other stakeholders such as those responsible for operating and maintaining the digital environment in order to better understand the key risk factors, such as the likelihood of certain ICT security threats, the prevalence of some ICT security vulnerabilities, the characteristics of some possible ICT security incidents (e.g. their potential for propagation and escalation) as well as the ICT measures which, among others, can support the treatment of the risk. While ICT experts can detect and address incidents at a technical level, they cannot analyse the economic consequences on the organisation of the incidents and of the technical measures taken to address it. Similarly, only leaders and decision makers can take into account digital security risk in the overarching strategic objectives and plans of the organisation.

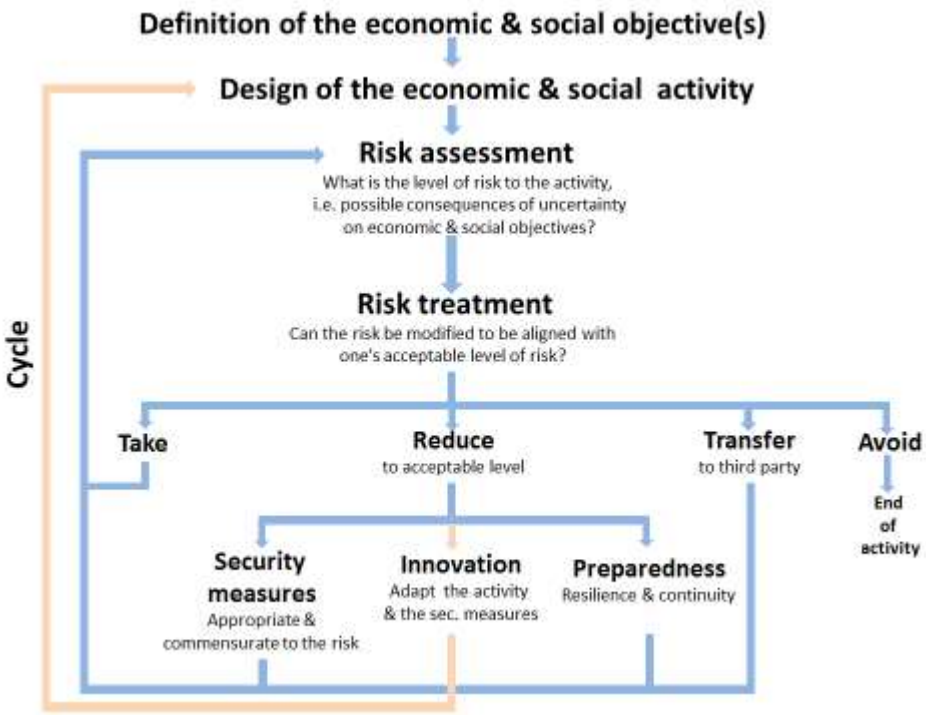
- *Ensures that "security measures" will fully support the economic and social activities at stake, and will not undermine them.* It is impossible to protect an activity against every potential threat, vulnerability and incident. Therefore, choices have to be made with respect to the selection and implementation of digital security risk management measures ("security measures"). Further, security measures are unlikely to be neutral with respect to the activity they protect. They can create different kinds of barriers and constraints for this activity. For example, they can increase financial cost, system complexity and time to market, as well as reduce performance, usability, capacity to evolve, innovation, user convenience. They can also generate privacy threats (see Box 4) and other adverse social consequences. These constraints and adverse effects can be addressed and mitigated, but at a cost. Digital security risk management roots security-related decisions in the economic and social reality of the activity at stake. It prevents decisions from being made in isolation, from a separate technical or security point of view. It drives the selection of "security measures" which are appropriate to, and commensurate with, the risk and activity at stake. In so doing, it ensures that the security measures will support the economic and social activities at

stake, and will not undermine them, for example, by inappropriately closing the environment or reducing functionality in a manner that would limit the possibility of taking advantage of ICTs to innovate and increase productivity.

- *Is an integral part of the overall risk management framework* rather than a separate and isolated silo. Digital security risk is one among many sources of risk to economic and social activities. Integrating digital security risk management to the broader organisation-wide risk management framework provides a better overarching picture of the risk landscape to higher-level leaders and decision makers, enabling more strategic and effective leadership and decision making. It would be counterproductive to create a specific risk management framework for digital security risk outside the existing risk management framework.

34. A typical risk management cycle should be an integral part of the decision making process related to the conduct of activities, and take place throughout these activities' lifecycle. Figure 1 provides a generic representation of risk management, reflecting the Operational Principles of the Recommendation. It starts with the definition of the objectives and design of the activities. The risk is then assessed and treated on the basis of this evaluation, in a manner that supports and preserves the objectives. Risk treatment determines whether and how the risk should be modified to increase the likelihood of success of the activities, that is deciding which part of the risk should be taken, reduced, transferred or avoided (Principle 1). To reduce the risk, security measures can then be selected and operated (Principle 2), innovation can be considered in relation to both the security measures and the activity at stake (Principle 3), and preparedness measures can be defined and applied when an incident happens (Principle 4). More details are provided in the section related to the Operational Principles.

Figure 1. Overview of the digital security risk management cycle



Source: OECD

Note: This figure, which reflects one possible representation among others of the risk management cycle, focuses on the Operational Principles of the Recommendation's Section 1. The General Principles should be considered as pillars supporting the cycle.

35. In relatively large organisations, the complexity of digital security risk management often requires the adoption of a formal framework to achieve comprehensiveness and consistency within the organisation. Generally reflected in a corporate or organisational policy or governance document, such a framework can take as many shapes as there are organisations' cultures and styles of management. It reflects the Principles of the Recommendation and is consistent with, and forms an integral part of, the organisation's overall risk management framework, where it already exists.

36. Such a framework is generally developed with the participation of all relevant actors and adopted at the highest level to ensure maximum consistency and visibility. This may raise complex governance issues which are not addressed in this paper, but would be useful to further analyse. Generally, the framework clearly articulates the responsibilities and accountabilities of the players in charge of implementing it. A key aspect that the framework can address is the modalities to ensure that the "business" and ICT leadership within the organisation work hand-in-hand to manage digital security risk.

37. The framework encompasses all aspects of the organisation's economic and social activities relying on the digital environment, throughout their lifecycle. It clarifies the organisational processes to ensure that risk is approached in an ongoing systematic manner. It is flexible to enable agile forward-looking responses to emerging digital security risk. As explained below (in the Operational Principles), the framework enables a holistic, systematic and flexible set of cyclical processes to be implemented with a view to coping with the inherently dynamic nature of risk. It takes good practices and standards into account while addressing context-specific elements which such practices and standards may not cover. A degree of transparency helps increase credibility and trust within and outside of the organisation by providing evidence of its commitment to address digital security risk. Such a framework should be easily and independently verifiable, for example by encouraging that the simple rule "write down what you do, do what you write down" is followed. An ongoing cycle of review and improvement of the framework is essential to ensure effective risk management and further increase trust. It generally includes processes to test, audit and optimise the measures in place.

38. Other details, such as regarding the cyclical nature of digital security risk management, are provided in the section addressing the Operational Principles.

Box 4. Digital security risk management and privacy

The relationship between digital security risk management and privacy protection has at least three facets.

First, digital security risk management provides a robust foundation for data controllers (i.e. the party who decides about the content and use of personal data) to implement the OECD Privacy Guidelines' Security Safeguards Principle which states that "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data".

In particular, digital security risk management helps ensure that the security measures are appropriate to and commensurate with the risk, which is an effective approach to defining "reasonable" security measures. However, the data controller may have a higher acceptable level of risk with respect to personal data than the data subject to whom the data relates. A key issue for privacy protection is this possible misalignment of the data controller's interests with those of the data subject. More generally, the fact that the party carrying out the risk assessment (the data controller) is not the one facing the risk (the data subject) is a major difference between security and privacy risk assessment.

In addition, digital security risk management could also undermine privacy, for example by establishing security measures which increase privacy risk, such as by monitoring networks, or sharing risk-related information with third parties, etc. Privacy protection is therefore included in the third Principle of the Recommendation's Section 1 on human rights and fundamental values, which calls for respecting and recognising the legitimate interests of others.

Finally, it is increasingly recognised that risk management may also be considered as a useful methodology to better implement the Privacy Guidelines' Principles. Nevertheless, more work is needed to understand practical applications and implications.

APPLICABILITY OF THE PRINCIPLES

39. The Principles should be implemented by stakeholders according to their "roles, ability to act and the context" (point IV). While this is generally valid for all the Principles, it is particularly important with respect to the Responsibility Principle and has consequences on the applicability of the Operational Principles.

Roles: distinguishing users from stakeholders responsible for the digital environment

40. As noted in the definition, stakeholders' roles can vary and be cumulated. An important distinction should be made between stakeholders in general and those who develop and diffuse digital goods and services. All stakeholders are users of the digital environment and, as such, should manage the digital security risk to their own activities. However, those among them who are in charge of developing and maintaining the digital environment (e.g. ICT professionals[26]) should also implement appropriate security measures in their goods and services, where possible[27], to empower their users to manage digital security risk. They should therefore develop a double culture of digital security risk management: the first one addressing risk to their own activities which rely on the digital environment, and the second aiming to optimise their goods and services to provide appropriate means to help consumers and users manage the risk related to their own use of the digital environment. They can, for example, design products and services in a way that enables consumers to understand and use security features that are "baked in" goods and services, user-friendly, and make appropriate use of defaults.

41. These two aspects are interrelated: failure to appropriately manage security risk related to the development of ICT goods and services can impact the effectiveness of the security measures embedded in these goods and services, thereby elevating the risk to users. For example, the information systems of the Dutch Certificate Authority DigiNotar were compromised in 2011, enabling attacks against 300 000 Gmail accounts, increasing security risk to DigiNotar's customers and affecting trust in the Dutch e-government infrastructure which indirectly relied on the company (which ultimately went bankrupt). Another example is the breach that took place at the security company RSA in 2011 which compromised about 40 million security tokens and enabled the use of stolen information to launch attacks on some of its customers in the defence sector.[28] Stakeholders in the ICT sector, and *a fortiori* in the ICT security sector, should be leading examples in the management of digital security risk.

Ability to act: distinguishing SMEs and individuals from other stakeholders

42. Stakeholders' ability to act can also vary significantly depending on, among other factors, *i)* their general understanding of digital security risk, *ii)* the amount of attention and resources they can allocate to this challenge, *iii)* their legal competence, sometimes called "authorisation" or "authority" to act, and *iv)* the degree to and ease with which they can control the digital environment. Regarding these four factors, governments and large organisations should be distinguished from SMEs and individuals whose ability to act can be generally regarded as more limited, especially for individuals. In particular, the degree of control that SMEs and individuals can exercise depends on the availability, affordability, usability and appropriateness of security measures in the digital goods and services they can find on the marketplace.[29]

43. Recognising these limitations, the Recommendation calls on governments and public and private organisations to work together to empower individuals and SMEs to manage digital security risk (point V). Furthermore, while they are conceptually relevant to all stakeholders, the Operational Principles in Section 1 have been drafted primarily to guide organisations beyond a certain size in the development of their digital security risk management framework. Further work is expected to be carried out after the adoption of the Recommendation to better understand the practical and public policy implications of these Principles for individuals and SMEs, and perhaps develop guidance in this respect.

The context: distinguishing specific situations

44. The context plays an important role in the interpretation of the Principles. Legal or regulatory requirements may for example influence how digital security risk management can be implemented, such as by requiring providers of critical services to carry out a formal risk assessment and demonstrate that appropriate measures are in place. In addition, while the Operational Principles require specific interpretation for SMEs and individuals on the basis of their limited ability to act, some of them operate in contexts that increase the importance of digital security risk management. Examples include SMEs involved in critical sectors, or individuals manipulating highly sensitive data, such as doctors or journalists.

45. It is worth noting that some individuals can act as stakeholders who develop and maintain elements of the digital environment outside of organisational structures. This is for example the case for some maintainers of key security components used by millions (e.g. OpenSSL, or GNU Privacy Guard (GPG)[30]) who sometimes work on these tools as volunteers or with very limited budget and support. It is also the case of a large majority of app developers, who according to a survey, earn less than USD 500 / month from their app.[31]

THE PRINCIPLES

Overall structure of the Principles

46. The eight Principles "should be taken as a whole"[32]: all are indispensable and each of them will be ineffective if interpreted or implemented in isolation, or if one of them is neglected. Their order and numbering reflects a logical narrative rather than an order of importance. The Principles are organised in two parts:

- General Principles (1 to 4) addressing "all stakeholders", that is governments, public and private organisations and the individuals who, directly or indirectly, rely on the digital environment for all or part of their economic and social activities.

- Operational Principles (5 to 8) addressing more specifically "leaders and decision makers" who, due to their highest level of leadership in government and in public and private organisations, are best placed to steer their organisation towards the adoption of an appropriate digital security risk management governance framework.

General Principles

47. Four Principles form the foundation on which an operational digital security risk management cycle can be established.

1. Awareness, skills and empowerment

48. Managing digital security risk requires first to understand that such risk exists and to acquire appropriate skills – through education, training, experience or practice – to make responsible decisions (empowerment). The first stage of a digital security risk management approach is therefore awareness raising and skills acquisition to empower stakeholders to manage risk.

49. Since all stakeholders are interdependent in the digital environment, the ignorance of the risk faced by one, or incapacity to manage it, can increase the risk for others.[33] Therefore, any awareness raising and skills development measures meant to empower a targeted audience also has a collective positive effect contributing to the overall reduction of the risk level, if that awareness and skills are effectively translated into action.

50. Awareness of risk is different from awareness of risk factors, i.e. threats, vulnerabilities and incidents. While the possible consequences of a car crash are intuitive – physical injury and death – the complexity of the digital environment blurs the link between an incident and its consequences. For example, many people are aware that their equipment can be infected by a virus, but do not necessarily understand the potential consequences such as identity theft, financial fraud or theft of trade secret. Consequences to others are even less visible, such as when an infected machine becomes part of a botnet used to launch denial of service attacks. Thus awareness raising should focus on the possible economic and social consequences (i.e. risk) of threats, vulnerabilities and incidents, rather than only on these risk factors. It should also encourage stakeholders to acquire appropriate skills to manage the risk in order to

best enjoy the economic and social benefits of the digital environment rather than dissuade them from using it.

51. Likewise, the development of the appropriate general culture for managing digital security risk is different from the awareness and skills that each participant should possess in order to assess and manage risk according to his/her role, ability to act and the context. It is essential to take into account the dynamic nature of the risk, risk factors, usage of the digital environment as well as economic and social activities at stake. Awareness raising and skills development is never ending. It requires an ongoing process integrated as part of the risk management cycle.

52. This Principle applies to all stakeholders: governments, public and private organisations and even individuals can increase digital security risk management awareness and contribute to elevating skills. Public and private organisations develop initiatives targeting their constituency to support their own risk management frameworks. Some of them, particularly businesses in the ICT sector as well as NGOs, play an important role by supporting awareness raising initiatives targeting the general public as well as specific audiences, such as children, teenagers, students, the elderly, etc. Initiatives can take many shapes and forms, using all types of media, courses, on-site training, etc. A key target audience – and a primary one for the Recommendation – is leaders and decision makers themselves, who are best placed to steer cultural and organisational changes within their organisation. In terms of public policy, considerable efforts have been made over the last ten years, both by governments and the private sector, to increase general awareness.[34] These efforts should continue to reach all categories of actors in the economy and society, and improve the acquisition of appropriate skills.

53. Sufficiently aware and skilled, empowered stakeholders can take responsibility (Principle 2).

2. Responsibility

54. It is a fundamental principle of social life that one should face the consequences of one's actions on oneself as well as on others. Thus all stakeholders should take responsibility for the management of digital security risk, according to their role, the context and their ability to act, as explained above.

55. This Principle does not address liability, that is the legal consequences of responsibility, which varies across legal regimes and contexts. Instead, the Responsibility Principle echoes the Recommendation's preamble which states that "governments, public and private organisations, as well as individuals share responsibility, based on their roles and the context, for managing digital security risk and for protecting the digital environment". It has become impossible to rely on someone else for all aspects of digital security risk management. Responsibility is shared: everyone has some degree of responsibility. All stakeholders should consider their role, the context, and their ability to act, and determine what responsibility they should take.

56. This responsibility underlines that the digital environment is not different from other environments: a certain level of digital security risk has to be accepted to achieve economic and social objectives.

57. To use an analogy, all stakeholders are also responsible vis-à-vis road safety, depending on their role, the context and their ability to act. Drivers should have learned how to drive and respect basic safety principles: not drink, respect speed limits, fasten their seat belt, taking other drivers into account, etc. Car manufacturers should design cars such that they minimise the possibility of accidents as possible due to design or mechanical failures (i.e. avoid vulnerabilities such as inadequate brakes) and embed protection mechanisms (i.e. insert safety measures such as airbags, rear mirrors, etc). Road builders should also design roads with the potential for accidents in mind: crash barriers, roundabouts, traffic lights, road signs,

etc. Governments should establish driving, car manufacturing, and road rules and enforce them. They should provide emergency services (i.e. preparedness measures). Failures at any point of these responsibilities increase the level of risk to each and all.

58. Stakeholders who decide to use the digital environment to achieve economic and social objectives (the drivers) are accepting a certain level of digital security risk – i.e. possible negative consequences. They should manage this risk, that is reduce it to an acceptable level on the basis of the four Operational Principles below. They should also be able to provide explanations about their actions or inactions (accountability).

59. However, not all participants are equal with respect to responsibility and accountability. They need to be able to manage the risk, for example in terms of information, knowledge, skills, resources, tools, and control, including regarding the technology. The ability of participants to identify, assess and manage risk varies substantially, and some types of participants (e.g. individuals and small enterprises) cannot reasonably be expected to identify, assess and manage risk like, for example, participants that have access to more significant resources. As noted above, further work regarding the challenges and possible avenues to facilitate the implementation of this Principle by individuals and SMEs would be most useful.

60. Stakeholders who develop, operate or manage components of the digital environment, such as software, hardware (i.e. the car manufacturers in the above analogy) and network infrastructures (i.e. road builders), should create the conditions for their users to make responsible risk management decisions. This includes, for example, adopting norms and good practices, embedding appropriate security measures in the technical components themselves and providing relevant information and assistance to empower users, taking into account the dynamic nature of the risk.

61. Governments, for their part, should develop national strategies and adopt public policy initiatives and measures to foster digital security risk management among all stakeholders. Most OECD governments already have many fundamental building blocks in place, such as regulations, legislation (e.g. on cybercrime, privacy), response capacity (through Computer Security Incident Response Teams, CSIRTs), education, public-private partnerships, etc. Several years ago they started to formulate their policies in more strategic terms[35] and to increase the consistency of their approaches, for example through new or improved co-ordination mechanisms such as dedicated agencies or other means. As reflected in Section 2, public policy for digital security risk management is inherently horizontal and requires co-operation not only within the government, but also with all stakeholders at domestic, regional and international levels. It is a long term strategic public policy effort.

62. However, in contrast with road safety, the degree of interconnection and interdependency between stakeholders is significantly higher in the digital environment. Thus the Responsibility Principle states that they should take into account the potential impact of their decisions on others. This relates, for example, to *i)* third parties whose personal data they process, *ii)* the overall digital ecosystem, which is in all stakeholders' shared interest to protect[36], and that their action or inaction may contribute to protect or degrade, and *iii)* the functioning of the economy and society as a whole, since the digital environment is used for critical infrastructures and services. Beyond adopting best practices and taking the interest of others into account, there are various other means to actively exercise collective responsibility: respect of standards and best practices and participation in standards bodies, collaboration with other stakeholders including across borders and disciplines, etc.

63. All stakeholders should also take responsibility for considering human rights and fundamental values as they manage digital security risk (Principle 3) and co-operate with others (Principle 4).

3. Human rights and fundamental values

64. Basic social rules apply to the digital environment. Therefore human rights and fundamental values extend to the digital environment and need to be protected in that environment. These rights and values are reflected in various international instruments, sometimes with other terms such as "core values", "fundamental freedoms", etc. Relevant international instruments in this area include the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and International Covenant on Economic, Social and Cultural Rights.[37]

65. Depending on how they are used, security measures adopted to manage digital security risk[38] can positively affect or undermine human rights and fundamental values. They can affect freedom of expression, the free flow of information, the confidentiality of information and communications, the protection of privacy and personal data, openness and fair process.[39] For example, security measures can enhance privacy protection, or provide anonymity to whistle-blowers and human rights activists. They can also enable the illegitimate monitoring of citizens, or prevent access to activists' content. They can affect other rights and values not listed in the Principle. Therefore, a responsible approach requires that decisions to manage digital security risk be made in light of their consequences on these rights and values.

66. This Principle applies to all stakeholders. Organisations should be aware that adoption of digital security measures which undermine human rights and fundamental values constitutes a risk to their image and credibility, and involves their legal responsibility. They should take advantage of the systematic nature of the digital risk management cycle to assess the impact of their security risk management decisions on human rights and fundamental values and adjust them as appropriate. The implementation of privacy management programmes, called for by the OECD Privacy Guidelines, could certainly benefit from being integrated into existing risk management frameworks and governance structures.[40]

67. Stakeholders who design, operate or manage the digital environment (e.g. ICT professionals) should consider whether security measures they include in ICT goods and services could be used to undermine human rights and take steps accordingly. In some cases, the potential impact on human rights depends on the context in which ICT goods and services are used and it may not be possible to prevent it by design. In such cases, ICT professionals should consider informing users of these goods and services about potential negative impact on human rights and how to prevent it. Finally, governments should ensure that their policies to foster digital security risk management support and respect legal and regulatory frameworks as well as their international obligations in this area (cf Section 2. A. 2).

68. Reflecting the so-called "Golden rule" or ethic of reciprocity ("one should treat others as one would like others to treat oneself"), stakeholders should also recognise that their action or inaction can harm others and affect the digital environment itself. As such, they should act in an ethical manner, i.e. respecting the legitimate interest of others and of society as a whole. Ethical conduct is particularly important considering that the open, global and interconnected nature of the digital environment can increase the impact of stakeholders' action or inaction.

69. Organisations should have a general policy of transparency about their practices and procedures to manage digital security risk. Guidance with respect to the modalities for implementing this general policy would however require further work, paying particular attention to the cases where too much transparency could undermine security as well as regarding possible oversight mechanisms.

4. Co-operation

70. As already highlighted, the global interconnectedness of the digital environment creates interdependencies among stakeholders. Interdependency has positive aspects such as enabling economic

and social benefits for each, based on the collective power of all. It has also drawbacks, such as increasing complexity, facilitating the propagation of threats and vulnerabilities, and potentially increasing collective risk. Since stakeholders are both interdependent and dependent on the digital environment, co-operation is essential.

71. Most aspects of digital security risk management require some degree of co-operation[41] and cannot be successfully addressed by an isolated party. Thus co-operation underpins all the other Principles of the Recommendation. For example: *i)* awareness and skills require the more aware and skilled to inform, educate and train others, who need to understand their interest in becoming more aware and empowered; *ii)* responsibility is shared among all stakeholders according to their role, ability to act and the context. Therefore, their co-operation is necessary for stakeholders with complementary roles to assume their responsibility in a coherent manner; and *iii)* although they are generally codified by law, human rights and fundamental values can be expressed in ethical terms and require dialogue and discussion among parties to be appropriately understood and respected. Co-operation is also key to the Operational Principles as their implementation requires extensive co-operation between the stakeholders responsible for carrying out economic and social activities and those responsible for providing the digital environment on which these activities rely. Co-operation is also essential for security measures, innovation and preparedness measures to be fully implemented, including with respect to non-technical aspects where humans have to modify their behaviour, and management processes have to be adopted to support digital security risk management.

72. Co-operation to better manage digital security risk should engage all stakeholders, taking into account their role. It should take place within organisations, transcending silos. The highest level of leadership can play a key role in ensuring that internal risk management policies and frameworks create the conditions for effective co-operation. A key aspect is co-operation between the parts of the organisation that use the digital environment for economic activities (the "business side"), those which provide that environment (the "ICT side"), and those which ensure legal and regulatory compliance.

73. Many other types of co-operation can be mentioned such as:

- Across organisations, for example to address the possible spread of threats and vulnerabilities among different companies and partners along the value chain. Similar concerns are shared within the government, for example across different ministries and agencies as well as levels of government (e.g. local/provincial/national), and contractors;

- Between organisations in the same economic sector which face common threats. In some cases, governments may encourage such co-operation, for example in the area of critical infrastructures;

- Between the public and the private sectors, such as for example, private sector co-operation with law enforcement, educational institutions, and other public bodies; and

- Between organisations and their consumers and users, and more generally the civil society.

74. With respect to public policy making, a multi-stakeholder approach is essential to create the conditions for broader engagement and development of better policies (Section 2.A.4). At a more practical level, it can take the form of public-private partnerships and initiatives in many areas, including awareness and skills, cybercrime (e.g. co-operation with law enforcement), CSIRT/CERT[42], information exchange and sharing[43], etc. Section 2 (in particular B.3, B.4) provides many examples of areas for public-private[44] co-operation.

75. Finally, co-operation should take place across borders, where appropriate.

Operational Principles

76. The overall cycle of digital security risk management was introduced in the "key concepts" part of this document. The elements below focus on each Principle. Nevertheless, as a general matter, it is important to understand digital security risk management as a creative and agile decision making process which can create opportunities for increased benefits through keeping an activity as responsive as possible to the ever changing – and therefore uncertain – context of its operation. It is **a dynamic response to a dynamic challenge** which provides the flexibility and adaptability to stakeholders to increase their likelihood of success. Thus digital security risk management is by nature:

- *Cyclical*: economic and social activities, the digital environment hosting them and digital security risks are constantly changing. Keeping pace ideally requires continuous review of the digital security risk. In practice, one should establish a general cycle driven by the activity as well as a more specific cycle driven by events such as the emergence of new threats and vulnerabilities, occurrence of new incidents, and evolution of other contextual aspects. The cyclical nature of risk management is represented in figure 1 by the arrows returning from the bottom to the risk assessment stage, and to the design stage in the case of innovation related to the activity.

- *Holistic*: since the digital environment is interconnected, the risk management approach should be comprehensive. For example, it should encompass the whole value chain of the activity at stake, as some vulnerabilities at one stage of the chain might be exploited by threats coming from another part of the chain and create consequences in a third point. It should also cover elements relating to humans (i.e. persons), processes (i.e. rules and procedures) and technologies involved along the value chain. It should therefore be managed together with the other categories of risk, without creating duplicative processes, or methodologies.

- *Systematic*: the complexity of a holistic risk management cycle is likely to reflect the complexity of the organisation and activities at stake. A systematic approach is the best way to manage the increasing complexity, by breaking down the various components and addressing them individually within the context of the whole.

77. The establishment of a cyclical, holistic and systematic digital security risk management approach creates the conditions for risk to be managed together with opportunities, as discussed below (Innovation Principle). It also provides a more comprehensive and appropriate approach for taking into account human rights and fundamental values, the legitimate interests of others, as well as the potential impact of security measures on human rights and fundamental values, and on the digital environment.

78. Various methodologies, standards and best practices can assist in carrying out risk management. They can help at many levels, for the overall process as well as for specific aspects such as security measures or preparedness.

5. Risk assessment and treatment cycle

79. Continuous risk assessment and treatment is essential to ensure that security-related decisions are appropriate to and commensurate with the risk and the economic and social activity at stake.

80. Risk assessment is *an analytical process* that can be broken down into several sub-stages whereby risk is *i)* identified: i.e. risk factors are recognised, often on the basis of experience, historical data, theoretical analysis, experts' views and opinions, etc.; *ii)* analysed: i.e. the risk is understood and the level of risk is determined. As noted above, this level is often expressed in terms of likelihood and impact

on the economic and social activity at stake; and *iii)* evaluated: i.e. the risk is compared to the acceptable level of risk relative to the activity and the economic and social objectives and benefits expected from it.

81. Although risk assessment should focus primarily on the potential consequences of uncertainty on one's objectives, it should also take into account, as appropriate, the potential consequences on others, to the extent that they play a role or could be affected (e.g. privacy, see Box 4). Risk assessment should also take into account the possible impact of uncertainty on the overall digital ecosystem (collective risk).

82. Risk treatment[45] is a *decision making process*, based on the output from risk assessment, regarding how to modify it to bring it to the acceptable level relative to the economic and social benefits expected from the activity, while taking into account the potential impact on the legitimate interests of others ("acceptable level of risk"). Such legitimate interests include human rights and fundamental values (Principle 3) as well as the functioning of the digital environment.

83. There are generally four possibilities to treat the risk (see Figure 1), which can be combined:

- Accepting it: "taking the risk" and accepting the effect of uncertainty on the objectives, including partial or complete failure. If the activity is undertaken, risk cannot be entirely eliminated, therefore some "residual" risk must be accepted (cf. Principle 2. Responsibility). In general, risk management is economically efficient when the benefits gained from carrying out the activity outweigh the residual risk.

- Reducing it to the acceptable level by *i)* selecting and applying security measures to protect the activities against certain potential threats exploiting vulnerabilities identified in the risk assessment (Principle 6), *ii)* changing the activity for example by redesigning or operating it differently, which can lead to innovation (Principle 7), and *iii)* defining and, as necessary, operating preparedness measures to cope with the occurrence of incidents (Principle 8).

- Transferring it: moving the unwanted effects of uncertainty on the activity's objectives to someone else, for example by contract such as through insurance. Digital security risk insurance might be a useful area for future work.

- Avoiding it: eliminating the risk by not carrying out the activity, or eliminating its digital element.

84. The "acceptable level of risk" is to be determined by the stakeholder who carries out the activity and faces the risk. The measure of how much risk the stakeholder is willing to accept to undertake an activity is known as its "risk appetite". It depends on many factors related to the activity and its objectives, as well as the culture and style of the organisation, market conditions, and technical environment, etc. It can also, in some cases, be limited by the legal and regulatory context. Unless risk is entirely accepted or avoided, a decision has to be made on how to reduce it to the acceptable level, or transfer it.

6. Security measures

85. Indispensable to protect economic and social activities, security measures can also have a negative impact on these activities. The Principle underlines that the best way to ensure that security measures are appropriate to and commensurate with the risk and the economic and social activity at stake is to select, implement and improve them on the basis of risk assessment and treatment (see above, definition of digital security risk management).

86. For example, security measures can increase the activity's cost, and affect its usability, performance, and potential for improvement. Many technical security measures can involve some degree of information flows' reduction (e.g. firewalls) or can impose additional steps in procedures (e.g. authentication). Some increase complexity (e.g. cryptography) and require trade-offs in terms of functionality to remain manageable. Examples of security measures which can potentially affect human rights and fundamental values include those which require access to personal data such as monitoring and analysing traffic flows to detect security threats (e.g. "deep packet inspection"). Security professionals are often exposed to personal data in the course of their work. For example, they may need to access personal accounts in order to analyse an incident. They may also need to transfer personal data related to an incident to third parties for further analysis or forensic investigations. Crisis management can also create situations whereby, for example, a service has to be taken down to reduce the propagation of a threat, potentially undermining users' rights. The digital security risk management cycle offers a systematic approach to ensure that such potential negative effects of security measures are taken into account and addressed through appropriate tools and practices.

87. Security measures, sometimes also called "mechanisms", "controls", or "safeguards", can be of very different natures: digital (e.g. security software), physical (e.g. locks, cameras, fences) or mixed (e.g. smart card); related to people (e.g. training), processes (e.g. organisational rule or practice) or technologies (e.g. cryptography); legal (e.g. contract), procedural (e.g. standards), managerial, etc. These are just examples of possible classifications.

88. Security measures also address vulnerabilities. Just as the threats are constantly changing, so are the vulnerabilities to the digital environment. Thus organisations should continually seek out, assess and appropriately address vulnerabilities as soon as possible, to stay ahead of new and emerging threats.

89. Since risk is dynamic, security measures should be selected when the activity is planned and they should be updated throughout the activity's lifecycle, following the cyclical, holistic and systematic approach explained above. Some measures should be embedded into the activity "by design", i.e. as a core component, for example because they are essential, or because the related part of the activity cannot be modified afterwards. However, since risk is dynamic, other security measures should be considered throughout the continuous risk assessment and management cycle.

90. Stakeholders who play a role in the design, management, and operation of the digital environment should always maintain good practices and follow standards with respect to security measures. Many general and sector-based standards and good practices can be applied to security measures. Following such standards can generally help address common aspects of security risk management, allowing the allocation of more time and resources to issues that are specific to the organisation or the activity.

91. Stakeholders who develop and maintain ICT goods and services should embed security measures in these goods and services and provide their users with the information and, as appropriate, the assistance they need to help them assess and treat the risks related to their use.

7. Innovation

92. In addition to adopting security measures, stakeholders can reduce their exposure to digital security risk by innovating with respect to the activity as well as the security measures. Innovation is generally defined as the implementation of a new or significantly improved product (good or service), or process (i.e. production or delivery methods), a new marketing method, or a new organisational method in business practices, workplace organisation or external relations.[46]

93. In the context of digital security risk management, innovation to reduce risk can take many forms which may or may not be related to digital aspects. For example, it may affect the organisation's economic or business model, processes such as payment methods, or even the redesign of physical, legal or other non-digital components of a product. Innovation introduced to reduce the possible effect of uncertainty on an activity can itself create uncertainties related to other aspects of the activity. It should therefore trigger a reassessment and treatment cycle.

94. Thus digital security risk management can become a driver for innovation, provided that it is approached as an integral part of the economic and social decision making processes related to an activity. When digital security risk management decisions are isolated from the core economic and social decision making process, it is more difficult to approach them as potential drivers for innovation. Instead, they may be viewed as inhibitors or imposed constraints rather than stimulus for competitive advantage.

95. In fact, risk, innovation and economic and social progress are highly interrelated. For example, one can relate many human inventions and progress throughout history to the willingness or need to manage uncertainty: climate uncertainties, for example, certainly led to the invention of the umbrella but also to considerable progress in agriculture, food storage, processing and distribution to reduce the risk of famine. Further work to better understand how risk and innovation are related in the digital environment would be useful.

96. From this perspective, the Principle can also be interpreted more broadly as a recognition that risk management can be viewed as a general approach to both preserve and create value. Risk management enables organisations to systematically respond to uncertainties in order to increase their likelihood of success in a constantly changing environment. However, as noted above, the effect of uncertainty is not necessarily detrimental to an activity. Risk has an upside and a downside: uncertainties can create opportunities to improve the activity as much as they can undermine it. Considering risk and opportunities as two facets of the same decision making coin, risk management can be viewed as a cycle whereby *i)* "negative risk" is assessed together with "positive risk" (i.e. the opportunities), and *ii)* risk treatment consists of deciding how to reduce the negative risk to an acceptable level, *as well as* to exploit the positive risk – i.e. seize opportunities – in order to best achieve the objectives. The integration of both aspects within a unique cyclical, holistic and systematic framework can increase organisations' agility and responsiveness, fostering their competitiveness and facilitating innovation.

97. This way of approaching risk management is relatively new[47] and further work would also be needed to better understand its potential benefits, and the obstacles to its generalisation, in particular with respect to digital security risk. Thus the Recommendation addresses the detrimental aspects of risk, as shown by the terms used to describe risk factors (e.g. threats, vulnerabilities and incidents) as well as the terminology related to "security" (e.g. availability, integrity,confidentiality) which relates to the realm of protection. Nevertheless, the Innovation Principle highlights that digital security risk management can also be viewed as a driver to exploit opportunities and foster innovation.

8. Preparedness and continuity

98. Digital security risk management is based on the recognition that it is impossible to provide a completely "safe and secure" digital environment where incidents are always avoided. Incidents can occur and affect economic and social activities, despite robust security measures being implemented and appropriately managed. Therefore digital security risk management is not limited to the deployment of security measures and innovation. It should also include a preparedness and continuity plan to define in advance the mechanisms that will reduce risk when incidents occur, by reducing their adverse effects on economic and social activities, and enabling continuity and resilience of these activities.

99. A preparedness and continuity plan should take into account the pace with which incidents can propagate and escalate in the digital environment. Stages of escalation are generally distinguished according to the scope and scale of consequences on the economic and social activities and objectives at stake. Various scales of escalation can be defined, such as Alert (no impact), Incident (impact only on IT), Emergency (limited economic and social impact), and Crisis (impact threatening the life of the organisation). Other terms and scales can be used, depending on the context. For example, public policy may consider the impact on a single organisation, its sector, the national economy as a whole, and beyond national borders. The allocation of responsibility should be different for each stage of escalation to ensure that the risk is appropriately managed during the incident. Here again, co-operation plays a key role in particular to ensure that both the economic and social effect of an incident as well as its technical aspects are understood by decision makers.

100. A preparedness plan should cover prevention, detection, response and recovery from digital security incidents. It should also provide for both individual and co-operative actions, such as appropriate exchange of information with other stakeholders, including between public and private sectors, and across national borders. It should be tested, assessed and reviewed in an ongoing cyclical manner to take into account the dynamic nature of risk. Computer Security Incident Response Teams (CSIRTs), also called Computer Emergency Response Teams (CERTs), can play a key role to assist stakeholders in their response to certain digital security incidents. Decision makers could benefit from internationally comparable statistical indicators reflecting the activity of CSIRTs/CERTs in view of better understanding the general level of risk.

101. Finally, appropriate notification procedures should be considered as part of the implementation of the plan. It may be voluntary in some cases or mandated by law in others.

ANNEX - POSSIBLE AREAS FOR FUTURE WORK

Possible areas for future work include:

- Digital security risk management governance in organisations: from a technical issue to a leadership priority;
- Risk management for privacy: learning from digital security risk management to better implement the OECD Privacy Guidelines. Exploring the commonalities, differences and synergies between digital security and privacy risk management, as well as the opportunities for a common framework;
- Relationship between innovation and digital security risk management, as well as applicability, benefits, and challenges to applying a "risk and opportunity" management approach to digital security issues (i.e. risk management for value protection *and* creation);
- Opportunities for and challenges to digital security risk management insurance;
- Interpreting the Principles for SMEs and individuals;
- Oversight in relation to digital security risk management;
- Guidance for public policy included in Section 2 of the Recommendation;
- International co-operation and developing economies;
- Improving the evidence base on digital security risk.

BIBLIOGRAPHY

ACMA (Australian Communications and Media Authority) (2011). An overview of international cyber-security awareness raising and educational initiatives. Available at www.acma.gov.au/theACMA/an-overview-of-international-cyber-security-awareness-raising-and-educational-initiatives.

Angwin, J. (2015). The World's Email Encryption Software Relies on One Guy, Who is Going Broke. Available at www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke.

App Promo (2012), Wake Up Call – If You Spend It, They Will Come. Available at http://app-promo.com/wake-up-call-infographic/.

App Promo (2013), App Promo White Paper. Slow and steady win the race. App Developers That Stick it Out Come Out on Top. App Promo Developer Survey June 2013. Available at http://app-promo.com/wp-content/uploads/2013/06/SlowSteady-AppPromo-WhitePaper2013.pdf.

Ashford W. (2013) Targeted cyber espionage on the increase, McAfee warns , available at http://www.computerweekly.com/news/2240185167/Targeted-cyber-espionage-on-the-increase-McAfee-warns.

Aven, T. (2012), The risk concept—historical and recent development trends. In Reliability Engineering & System Safety Volume 99, March 2012, Pages 33–44 http://dx.doi.org/10.1016/j.ress.2011.11.006.

Dark Reading (2012), 4 Long-Term Hacks That Rocked 2012. Available at www.darkreading.com/application-security/database-security/4-long-term-hacks-that-rocked-2012/d/d-id/1138643.

Fechner, B. (2014), Les entreprises françaises face au défi de l'espionnage industriel. Available at http://lexpansion.lexpress.fr/actualite-economique/les-entreprises-francaises-peuvent-elles-relever-le-defi-de-l-espionnage-industriel_1633978.html.

CBC News (2012), Nortel collapse linked to Chinese hackers. Available at www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591.

Choe, S. (2014), Theft of Data Fuels Worries in South Korea. Available at www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html.

Chung E. (2015), Autonomous Cars could save Canadians $65B a year. Available at www.cbc.ca/news/technology/autonomous-cars-could-save-canadians-65b-a-year-1.2926795.

CIGI (Centre for International Governance Innovation) (2014), CIGI-Ipsos Global Survey on Internet Security and Trust. Available at https://www.cigionline.org/internet-survey.

CNIL (Commission Nationale de l'Informatique et des Libertés), (2012), Methodology for privacy risk management. Available at www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf.

Council of Europe (2001), Convention on Cybercrime. Available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

ENISA (European Union Agency for Network and Information Security) (2013), National Cyber Security Strategies in the World. Available at www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

ENISA (n.d.), Existing Taxonomies. Available at www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies.

Europol (2013), Notorious Botnet Infecting 2 Million Computers Disrupted. Available at www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted-0.

Gaudiosi, J. (2014), Why Sony didn't learn from its 2011 hack. Available at http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

ISOC (Internet Society) 2015, Collaborative Security: An approach to tackling Internet Security issues. Available at www.internetsociety.org/collaborativesecurity.

Jackson, W. (2014), Cyber Espionage Incidents Triple: Verizon Report. Available at www.informationweek.com/government/cybersecurity/cyber-espionage-incidents-triple-verizon-report/d/d-id/1204612.

Kim Y. (2014), Top executives resign over massive data leak. Available at www.koreaherald.com/view.php?ud=20140120001002.

Kitten T. (2014), Chase's Cybersecurity Budget to Double. Available at www.bankinfosecurity.com/chases-cybersecurity-budget-to-double-a-7427.

Lee R., Assante, M., Conway, T. (2014), German Steel Mill Cyber Attack. Available at https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

Leyden J. (2013), Biggest DDoS attack in history hammers Spamhaus. Available at www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood.

Molla R. (2012), Most app developers make less than $500 a month. Available at https://gigaom.com/2012/10/04/most-app-developers-make-less-than-500-a-month-chart/.

NACD (National Association of Corporate Directors) (2014), NACD Reports Directors Dissatisfied with Cyber and IT Risk Information. Available at www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=12530.

NIST (National Institute of Standards and Technology) (2012), Guide for conducting risk assessment. Special publication 800-30, revision 1. Available at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

NIST (2014), Framework for Improving Critical Infrastructure Cybersecurity. Available at www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

O'Connor C. (2014), Target CEO Gregg Steinhafel Resigns in Data Breach Fallout. Available at www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout.

OECD (2002), Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security. Available at http://www.oecd.org/internet/ieconomy/15582260.pdf.

OECD/Eurostat (2005), Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd Edition, The Measurement of Scientific and Technological Activities, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264013100-en.

OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures. Available at http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117.

OECD (2011), Recommendation of the Council on Principles for Internet Policy Making. Available at http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=270&InstrumentPID=275.

OECD (2012a), Connected Minds: Technology and Today's Learners, Educational Research and Innovation, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264111011-en.

OECD (2012b), ICT Applications for the Smart Grid: Opportunities and Policy Implications", OECD Digital Economy Papers, No. 190, OECD Publishing. Available at http://dx.doi.org/10.1787/5k9h2q8v9bln-en.

OECD (2012c), "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", *OECD Digital Economy Papers*, No. 214, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5k4dq3rkb19n-en.

OECD (2012d), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OECD (2013a), *The Internet Economy on the Rise: Progress since the Seoul Declaration*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264201545-en.

OECD (2013b), ICTs and the Health Sector: Towards Smarter Health and Wellness Models, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264202863-en

OECD (2013c), Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Available at http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False.

OECD (2014), Recommendation on Digital Government Strategies, available at www.oecd.org/gov/public-innovation/recommendation-on-digital-government-strategies.htm.

OSCE (2013), Decision no. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Available at www.osce.org/pc/109168.

Peters, S. (2014), Pharmaceuticals, Not Energy, May Have Been True Target Of Dragonfly, Energetic Bear. Available at www.darkreading.com/pharmaceuticals-not-energy-may-have-been-true-target-of-dragonfly-energetic-bear/d/d-id/1316869.

Piper, A. (2014), Risk-informed innovation. Harnessing risk management in the service of innovation. The Economist Intelligence Unit. www.economistinsights.com/technology-innovation/analysis/risk-informed-innovation.

Prince, B. (2014), Incident Response Plans Lacking in Many Organizations: Survey. Available at www.securityweek.com/incident-response-plans-lacking-many-organizations-survey.

Rawlinson, K. (2015), Charlie Hebdo: 'Islamist cyber attacks' hit France. Available at www.bbc.com/news/technology-30850702.

SecurEnvoy (2012), The RSA Security breach – 12 months down the technology turnpike. Available at www.securenvoy.com/blog/2012/04/27/the-rsa-security-breach-12-months-down-the-technology-turnpike/.

United Kingdom Cabinet Office (2011), The cost of cybercrime, available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

United Nations (1948), Universal Declaration of Human Rights. Available at www.un.org/en/documents/udhr/.

United Nations (1966a), International Covenant on Civil and Political Rights. Available at www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

United Nations (1966b), International Covenant on Economic, Social and Cultural Rights. Available at www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx.

United Nations (2003), Creation of a global culture of cybersecurity. Resolution adopted by the General Assembly A/RES/57/239. Available at www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239.

United Nations (2013), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

Westby J. (2012), Governance of Enterprise Security: CyLab 2012 Report. How Boards & Senior Executives Are Managing Cyber Risks. Available at http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.

Yadron D. (2014), Internet Security Relies on Very Few. Available at www.wsj.com/news/articles/SB10001424052702303873604579495362672447986.

NOTES

1 Such as energy, see OECD, 2012b, transports, manufacturing, etc.

2 See OECD, 2013b.

3 See OECD, 2012a.

4 See www.oecd.org/about/whodoeswhat

5 See www.oecd.org/sti/ieconomy.

6 See www.oecd.org/legal/legal-instruments.htm.

7 Respectively represented by the Business and Industry Advisory Committee to the OECD (BIAC), the Civil Society Information Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC).

8 E.g. the predecessor of this Recommendation (the 2002 Security Guidelines) was referenced in ISO 27001:2002 and inspired the United Nations Resolution 57/239 (United Nations, 2003).

9 Council of Europe , 2001. See also Cybercrime Programme Office of the Council of Europe (C-PROC) at www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp .

10 See www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

11 See for example United Nations, 2013.

12 See OSCE, 2013.

13 In particular through its Telecommunications and Information Working Group (APEC TEL).

14 For example local, regional, provincial, federal, etc. See below explanations about « Stakeholders and their roles ».

15 See the part of the Companion document on the "Applicability of the Principles" for more details on the notions of roles, ability and context.

16 CNIL, 2012, p. 13.

17 See for example Dark Reading, 2012 which provides examples of long term attacks at the US Chamber of Commerce, Nortel, Coca-Cola and the Japanese Ministry of Finance. Nortel's bankruptcy was reportedly related to digital espionage and in particular a 10 year long stealth intrusion in the company's information system. See CBC News, 2012.

18 See for example Europol, 2013.

19 See OECD, 2012d, and ENISA, 2013.

20 A 2012 survey of 108 respondents from Forbes Global 2000 companies found that 57% of respondents are not analysing the adequacy of cyber insurance coverage or undertaking key activities related to cyber risk management to help them manage reputational and financial risks associated with the theft of confidential and proprietary data and security breaches. Westby, 2012. See also NACD, 2014 and Prince, 2014.

21 CIGI, 2014: 78% of users are concerned about a criminal hacking into their personal bank accounts. 77% of users are concerned about someone hacking into their online accounts and stealing personal data. 72% of users are concerned about institutions in their country being cyber-attacked by a foreign government or terrorist organization

22 There might also be intersections here when the breach of intellectual property happens as a consequence of a security incident (e.g. the penetration of an organisation's information system to obtain confidential

industrial or trade secrets, or the dissemination of illegal content (e.g. hate speech) through the defacement of a web site.

23 For example, in "if you cross the street, there is a risk of being hit by a car", risk points to an event or incident; in "cars are a risk for pedestrians when they cross the street", risk points to a threat or danger; and in "there is a risk that you die if you don't pay attention when you cross the street", risk points to the consequence of the incident.

24 There are many risk-based standards and methodologies from various national, regional and international bodies, both governmental, and non-governmental, with a general or sectorial (e.g. finance, public administration, etc.) approach. For example, the European Union Agency for Network and Information Security (ENISA) lists 17 of them at http://rm-inv.enisa.europa.eu/methods and there are others such as the US NIST 800-30 Rev. 1 Guide for conducting risk assessments (NIST, 2012) and more recent Cybersecurity framework (NIST, 2014). Standards often reflect different perspectives and address different audiences, use different terms and definitions, without necessarily being inconsistent with the Recommendation. For example, the term "risk treatment" might be called "risk mitigation" in some standards, and in some others "risk reduction" can be called "risk mitigation", "risk avoidance" can become "risk termination", and "vulnerability" transform into a "weakness", etc.

25 Aven, T. (2012).

26 "ICT professionals" may include individual stakeholders who are not practicing ICT skills as their main profession, as it is the case for a large number of app developers.

27 In some cases, the technical complexity of an issue may mean that while it may be possible for the digitial security risk to be reduced, it may not be done in a way that enables the individual to be empowered to control it. For example, network services and other remotely delivered services will implement security solutions centrally.

28 SecurEnvoy, 2012.

29 The marketplace should be understood in the broad sense of where supply and demand meet. It includes free and open source software.

30 See Angwin, 2015, Yadon, 2014.

31 "68% of survey respondents indicated their app has earned less than $1,000 since launch with 29% of the respondents indicating that their app has yet to generate any income at all" (App Promo, 2013). "Most app developers make less than $500 a month" (Molla, 2012). See also App Promo, 2012.

32 Cf. point VI: [The Council] "Agrees that the Principles are complementary and should be taken as a whole…".

33 For example, an infected computer or device can be used to attack someone else's assets (e.g. in distributed denial of service attacks) and the disclosure of personal data through a security attack can impact the lives of the individuals whose data has been stolen in addition to the economic interest of the organisation facing the incident.

34 For an international comparative analysis of initiatives, see ACMA, 2011.

35 OECD, 2012d.

36 The « Mindful » statement of the Recommendation's preamble (10th paragraph) underlines that stakeholders share responsibility for protecting the digital environment. For more details on the notion of "collective responsibility", see ISOC, 2015.

37 United Nations, 1948, 1966a and 1966b.

38 It is important to underline that the Recommendation uses the expression "security measures" to cover security measures for digital security risk management. Other types of security measures are beyond its scope.

39 The Communiqué explaining the principles contained in the 2011 Recommendation of the Council on Principles for Internet Policy Making states that "[…] It is clear that the open and accessible nature of the Internet needs to be supported for the benefit of freedom of expression, and to facilitate the legitimate sharing of information, knowledge and exchange of views by users, including research and development, that has brought about widespread innovation to our economies […]". The 2011 Recommendation itself "Recommends that, in developing or revising their policies for the Internet Economy, Members, in co-operation with all stakeholders, take account of the following high level principles [:] […] Ensure transparency, fair process, and accountability". On this point, the Communiqué further explains that "In order to build public trust in the Internet environment, policy-making processes and substantive policies that ensure transparency, fair process, and accountability should be encouraged. Transparency ensures that Internet users have timely, accessible, and actionable information that is relevant to their rights and interests. Fair process provides predictable decision-making procedures to govern the definition, assertion, and defence of rights. Accountability is achieved through policies that make parties answerable, where appropriate, for their actions on the Internet."

40 OECD 2013c, Part Three, para 15 a).

41 Co-operation was highlighted in the 2002 Security Guidelines as a useful concept. It became a Principle in this Recommendation to underline its increased relevance and essential role to support the other Principles.

42 An interesting example is CONCERT, a Korean Consortium of CERTs created in 1996 to exchange and share information and cooperate with partners on issues of common interest related to security. It gathers over 300 corporate information security units, relevant institutes and governments in Korea. See www.concert.or.kr.

43 Such as the UK Cyber-security Information Sharing Partnership (CiSP). See www.cert.gov.uk/cisp.

44 In the expression "public-private", the term "private" includes stakeholders which do not belong to the public sector such as businesses, non-profits, civil society, academia, the technical community, etc.

45 Risk "treatment" is sometimes called differently, such as risk "mitigation". See box on terminology and definitions. Example of other terms related to risk treatment include: accepting, taking or assuming risk; reducing, mitigating or minimising it; transferring or re-allocating it; avoiding or terminating it.

46 OECD/Eurostat, 2005.

47 Piper, 2014.