Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity

OECD Legal Instruments

OECD
BETTER POLICIES FOR BETTER LIVES

Please cite this document as:
OECD, *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*, OECD/LEGAL/0415

Series: OECD Legal Instruments

Date(s)

Adopted on 17/09/2015

Background Information

The Recommendation on Digital Security Risk Management for Economic and Social Prosperity was adopted by the OECD Council on 17 September 2015 on the proposal of the Committee on Digital Economy Policy. This Recommendation replaces the 2002 Recommendation on the Security of Information Systems and Networks: Towards a Culture of Security. It provides guidance for a new generation of national strategies on the management of digital security risk aimed to optimise the economic and social benefits expected from digital openness. At time of adoption, this Recommendation was the only international instrument on “cybersecurity” developed from an economic and social perspective. Together with the OECD Privacy Guidelines revised in 2013 it forms a robust basis for a better international dialogue on trust in the digital economy.

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. Responsability

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) Fostering 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;

IX. **INVITES** non-Members to adhere to this Recommendation;

X. **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.

Adherents*

OECD Members		Non-Members
Australia	United States	Brazil
Austria		Peru
Belgium		
Canada		
Chile		
Czech Republic		
Denmark		
Estonia		
Finland		
France		
Germany		
Greece		
Hungary		
Iceland		
Ireland		
Israel		
Italy		
Japan		
Korea		
Latvia		
Lithuania		
Luxembourg		
Mexico		
Netherlands		
New Zealand		
Norway		
Poland		
Portugal		
Slovak Republic		
Slovenia		
Spain		
Sweden		
Switzerland		
Turkey		
United Kingdom		

*Additional information and statements are available in the Compendium of OECD Legal Instruments: http://legalinstruments.oecd.org

About the OECD

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD Member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Legal Instruments

Since the creation of the OECD in 1961, around 450 substantive legal instruments have been developed within its framework. These include OECD Acts (i.e. the Decisions and Recommendations adopted by the OECD Council in accordance with the OECD Convention) and other legal instruments developed within the OECD framework (e.g. Declarations, international agreements).

All substantive OECD legal instruments, whether in force or abrogated, are listed in the online Compendium of OECD Legal Instruments. They are presented in five categories:

- **Decisions**: OECD legal instruments which are legally binding on all Members except those which abstain at the time of adoption. While they are not international treaties, they entail the same kind of legal obligations. Adherents are obliged to implement Decisions and must take the measures necessary for such implementation.

- **Recommendations**: OECD legal instruments which are not legally binding but practice accords them great moral force as representing the political will of Adherents. There is an expectation that Adherents will do their utmost to fully implement a Recommendation. Thus, Members which do not intend to do so usually abstain when a Recommendation is adopted, although this is not required in legal terms.

- **Declarations**: OECD legal instruments which are prepared within the Organisation, generally within a subsidiary body. They usually set general principles or long-term goals, have a solemn character and are usually adopted at Ministerial meetings of the Council or of committees of the Organisation.

- **International Agreements**: OECD legal instruments negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.

- **Arrangement, Understanding and Others**: several ad hoc substantive legal instruments have been developed within the OECD framework over time, such as the Arrangement on Officially Supported Export Credits, the International Understanding on Maritime Transport Principles and the Development Assistance Committee (DAC) Recommendations.