Chapter 14

Digital security risk management

This chapter focuses on public policies to manage digital security. It first distinguishes digital security risk management from other aspects of cybersecurity related to technology, law enforcement, national security and defence. Next, it introduces the key elements of national strategies that can create framework conditions to increase trust for all stakeholders using ICTs, and for the digital environment for economic and social prosperity. The chapter surveys existing measurement and impact assessment tools and provides an overview of public policy efforts in the LAC region. Finally, it introduces selected good practices.
Broadband and information and communication technologies (ICTs) in general have become essential to the development and functioning of the economy in many areas in the Latin American and Caribbean (LAC) countries, in particular for critical infrastructure such as energy, transport, water, finance and key government services. However, the economic and social benefits of broadband policies can only be realised if stakeholders manage digital security risk, that is, the security risk associated with the use of the digital environment.

Many LAC countries have developed policies that address some aspects of digital security. However, they generally do not address this issue from a strategic perspective, with a clear vision for the future. Most importantly, they generally do not approach cybersecurity policy as a means of increasing economic and social prosperity, focusing instead on the technical and criminal aspects of the issue, or on national security. The policies in place often lack the appropriate level of co-ordination between the governmental and stakeholders. This undermines public policy efforts to encourage the use of ICTs, as a result of a limited understanding of the economic and social dimensions of cyber security.

This section presents a set of policy concepts and instruments to help develop policies for managing digital security risk for economic and social prosperity. It provides an overview of the situation in the LAC region, points to good practices in these countries and establishes recommendations based on the OECD 2015 Recommendation on Digital Security Risk Management for Economic and Social Prosperity (OECD, 2015a), as well as the work of other international and regional organisations, such as the Inter-American Development Bank (IDB) and the Organization of American States (OAS).

Key policy objectives in the LAC region

The main high-level policy objective for the adoption of a national strategy for managing digital security risk is to create framework conditions for all stakeholders to use ICTs and the digital environment for economic and social prosperity. This general policy involves certain key objectives:

- **Understanding digital security and stakeholders’ responsibility for managing it.** All stakeholders should be aware that digital security risk can affect their economic and social welfare and that their management of digital security can affect others. Stakeholders should be equipped with the education and skills to understand risk and to manage it. In particular, they should understand that digital security risk management is an economic and social challenge, not simply a technical or national security issue.

- **Developing a national strategy for the management of digital security risks.** National strategies for the management of digital security risk should aim to promote economic and social prosperity. They should be co-ordinated broadly within the government to ensure consistency with other strategies for economic and social prosperity, and coherence with policies intended to protect critical infrastructure and ensure the provision of essential services. The aim is to combat criminality, protect national security and preserve international stability. These strategies should be supported at the highest level
of government, to ensure that the various interests at stake are appropriately balanced. They should be flexible and technologically neutral, and meanwhile, preserve and protect human rights and fundamental values.

- **Engaging with other stakeholders.** Policy makers should encourage the active participation of all stakeholders, from business, civil society, the Internet technical community and academia, in developing and implementing strategy and policy.

- **Cultivating international co-operation and mutual assistance.** Policy makers should establish multilateral and bilateral relationships to share experiences and good practices and promote an approach to digital security risk management that does not increase risk to other countries.

### Tools for measurement and analysis in the LAC region

There are a limited number of references on key performance indicators and measurements for policy makers in the area of digital security risk management. These include the ITU Global Cybersecurity Index (ITU, 2014), the Cybersecurity Capability Maturity Model of the Oxford-based Global Cybersecurity Capacity Centre (2014), the Business Software Alliance (BSA) Cybersecurity Dashboard (BSA, 2015), and, in the area of energy, the US Department of Energy’s Cybersecurity Capability Maturity Model (C2M2) Program (US Department of Energy, 2015). However, these generally approach cybersecurity as a technical issue rather than an economic and social challenge. Work is currently under way at the national level in some countries and in international forums to improve the evidence base for public policy in this area. OECD recommendations and examples of good practices on specific areas, measurement of security and privacy issues in the context of children’s online access, and on Computer Security Incident Response Teams (CSIRTs) are available in the documents referenced below (Box 14.1).

### Box 14.1. OECD references on measurement in the area of digital security


This report provides an overview of the existing data and statistics in the fields of information security, privacy and the protection of children online. It highlights the potential for developing better indicators in these fields, showing that a wealth of empirical data exists that, if mined and made comparable, will enrich the current evidence base for policy making. Such indicators would help identify areas where policy interventions are most clearly warranted, and can provide guidance on designing policy interventions and determining their effectiveness.

Starting from a broad scope covering all aspects of security and privacy, the report identifies the “low-hanging fruit”, or areas where better indicators could be immediately developed with minimal resources. They include:

- improving the relevance of the OECD model surveys on ICT use by businesses and households/individuals for policy makers in the areas of information security, privacy and in particular the protection of children online

- improving the cross-country comparability of statistics provided by national/government CSIRTs in the area of information security, and privacy enforcement authorities (privacy authorities) in the area of privacy.
Overview of the situation in the LAC region

National digital security strategies

Only six countries (Colombia, Mexico, Panama, Paraguay, Trinidad and Tobago and Uruguay) have a national digital security strategy, two of which (Mexico and Uruguay) address a national government strategy but not a digital security strategy per se.

Although 75% of countries in the LAC region still do not have a digital security strategy, a large number of countries, including Argentina, Brazil, Chile, Mexico and Paraguay, have government and public sector entities responsible for the co-ordination and protection of national security and critical infrastructure (OAS and Symantec, 2014).

The OAS has provided support and technical assistance to Costa Rica, Jamaica (OAS, 2015b), Paraguay and Peru in the implementation and improvement of their respective national digital security strategies (OAS, 2015a, 2015b, 2015c and 2015d).

A recent cybersecurity study (IDB and OAS, 2016) analysed the state of preparedness of 32 countries in the region based on 49 indicators in five areas: policy and strategy, education, culture and society, legal framework, and technology. Uruguay, Brazil, México, Argentina, Chile, Colombia and Trinidad and Tobago have achieved an intermediate level of preparedness, but lag advanced countries like the United States, Israel, Estonia and Korea.
The proportion of LAC countries with both substantive and procedural legislation to investigate and prosecute Internet and computer-related crime is still low (nearly 44%). Only 11 countries (Chile, Colombia, Costa Rica, the Dominican Republic, Jamaica, Mexico, Paraguay, Peru, Trinidad and Tobago, Uruguay and Venezuela) have substantive and procedural criminal legislation to counter cybercrime. However, some countries have reported problems not only with the enforcement of laws and concerns on how to keep cybercrime legislation up to date, but the need for training prosecutors and the judiciary to build capacity for law enforcement, given the knowledge gap among experts, as well as budget constraints (IDB and OAS, 2014).

Most government agencies of countries in the region tend to view digital security exclusively from one dimension (i.e. political, technical, industry-specific) rather based on a multidimensional perspective (IDB and OAS, 2014). Few place emphasis on the economic and social dimensions. As a result, governments do not sufficiently use public-private partnerships and co-operation to advance public policy objectives in this area.

**Intra-governmental co-ordination**

The proportion of LAC countries with government co-ordination mechanisms is very low (around 30%). Only eight countries (Brazil, Colombia, the Dominican Republic, Jamaica, Mexico, Peru Trinidad and Tobago and Uruguay) address some aspects of governmental co-ordination for developing their national digital security strategy. However, the information provided suggests that intra-governmental co-ordination is limited in practice and that most LAC countries do not yet have a whole-of-government approach to digital security risk.

OAS member countries have reported problems of co-ordination and alignment of digital security policies throughout government agencies. It is reported “a general lack of collaborative culture, which combined with budget constraints, makes the co-ordination of digital security policies a great challenge within government”. Other OAS members reported a fragmented approach on digital security matters within their governments, with independent institutions working in an isolated rather than in a co-ordinated fashion (IDB and OAS, 2014).

**Computer Security Incident Response Teams (CSIRTs)**

The proportion of LAC countries with a computer security incident response team (CSIRT) fully endorsed by the government is relatively high (more than 50%). Twelve countries (Argentina, Brazil, Chile, Colombia, Costa Rica, Guatemala, Jamaica, Mexico, Paraguay, Peru, Trinidad and Tobago and Uruguay) have a CSIRT fully endorsed or supported by its national government.

The Inter-American Committee Against Terrorism of the OAS (CICTE) has been working closely with all countries in the Americas on establishing and improving their incident response capabilities under OAS’ *Programme for Developing a National Computer Security Incident Response Team*. Under this programme, the number of national CSIRTs in the Americas has increased from 5 to 18. However, according to reports, “the lack of financial resources and of personal training are the major challenges for implementing a national CERT and improving countries’ response capacity to cyber threats in the Americas” (IDB and OAS, 2014).

**Awareness and development of a skilled workforce that can manage digital security risk**

Many countries in the LAC area have increased and improved their awareness-raising activities to enhance digital security and counter cybercrime (Box 14.2). “Stop. Think. Connect”, a multi-stakeholder partnership initially launched in October 2010 to help digital citizens stay safer and more secure online, continues to expand, and now includes four LAC
government authorities (the Dominican Republic, Jamaica, Panama, Paraguay and Uruguay), CICTE and other private and public organisations in the region.\footnote{1}

The OAS recently launched an Awareness Campaign Toolkit on Cybersecurity, designed to provide governments and organisations guidance and resources in developing a cybersecurity awareness campaign (OAS, 2015e). However, capacity and training in countries in the region is often limited to the technical perspective. Training and capacity does not yet include skills to manage digital security from a broader perspective.

**Box 14.2. Digital security awareness programmes**

**Mexico: National programme on public security**

Mexico has implemented a National Programme on Public Security (Programa Nacional de Seguridad Pública 2014-2018). Section 4.2.9 establishes as a policy objective: “To encourage a culture of cybersecurity, particularly among children and teenagers, to prevent them from falling prey to Internet crime”.


**Mexico: National Cyber Security Week**

In October 2015, as part of public awareness activities on digital security, Mexico’s Ministry of the Interior (SEGOB), the National Security Commission of the Federal Police (PF) and the OAS organised the National Cyber Security Week, holding a series of conferences, seminars and training activities on information security to counter cybercrime at the national level.


**Peru’s campaign to improve security of government information**

Peru’s national CERT (Pe-CERT) disseminates information to increase and improve security levels of national information systems and networks and provides regular training and capacity on ICTs.


**Uruguay: Seguro te conectas national campaign**

Uruguay’s national CERT (CERT-Uy) organises conferences and information-security training simulations and has promoted national awareness campaigns like “Seguro te conectas”. This promotes responsible use of the Internet with a number of audiovisual recommendations and good practices to raise public awareness of the risks of misuse of ICTs.

Source: CERT-Uy and information on the “Seguro te conectas” campaign, www.cert.uy/Seguro-te-conectas/.

**Building a comprehensive legal framework to mitigate cybercrime**

The Dominican Republic and Panama are the only LAC countries that have ratified the 2001 Budapest Convention on Cybercrime (CoE, 2016), although the Council of Europe has officially invited seven other LAC countries (Argentina, Chile, Colombia, Costa Rica, Mexico, Paraguay and Peru) to sign (CoE, 2014).

Nevertheless, the proportion of LAC countries that have adopted substantive and procedural legislation in line with the Budapest Convention keeps growing (nearly 43%). Eleven countries (Chile, Colombia, Costa Rica, the Dominican Republic, Jamaica, Mexico, Paraguay, Peru, Trinidad and Tobago, Uruguay and Venezuela) have passed legislation to counter cybercrime. The cases of the Dominican Republic and Panama are noteworthy (Box 14.3).
Box 14.3. **Selected countries that have ratified the Budapest Convention**

**Dominican Republic**

The Dominican Republic was one of the first LAC countries to pass an independent law to investigate, prosecute and punish cybercrime under the substantive, procedural and international co-operation provisions of the Budapest Convention (Law No. 53-07 on Crimes and High-Tech Crime) in force since 18 January 2007. The Dominican Republic was the first LAC country to ratify the Budapest Convention, on 7 February 2013.

*Source: Dominican Republic (2007), Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, www.oas.org/juridico/PDFs/repdom_ley5307.pdf.*

**Panama**

Panama was the second LAC country to ratify the convention, on 1 July 2014. It does not yet have an independent law to investigate, prosecute and punish cybercrime, but a draft bill to reform the Criminal Code is pending approval by the National Assembly. The draft bill includes the criminalisation of conducts and crimes committed through information technologies, in line with the Budapest Convention’s provisions.

---

**Allocation of budget and resources to set up a digital security strategy**

As addressed in Chapter 2 on regulatory frameworks and digital strategies, the great majority of LAC countries have an annual budget allocation for a national digital strategy, although the budget varies significantly from one country to another. Mexico’s National Digital Strategy has an annual budget of USD 1.740 million (MXN 29 million), while Colombia allocated nearly USD 2.6 million for the first three years of its National Digital Strategy (Vive Digital). Chile budgeted USD 850 million for its National Digital Strategy. Nevertheless, the percentages dedicated to digital security are unclear.

Besides the general annual budget for national digital strategies, specific ministries can also allocate their own budgets for the digital security strategy. This is not common, however, in most LAC countries. In 2014, only Colombia allocated an annual budget to the National Defence Ministry equivalent to USD 1.5 million (COP 4.6 million) for colCERT, the Cybercrime Police Centre (CCP) and the Cyber Task Force of the Armed Forces.

Most recently, Mexico’s Ministry of National Defence requested an annual budget of USD 100 million to create a Cyberspace Operation Centre in 2016. Its main purpose would be to build strategic capacity and training to counter cybercrime, threats to information security and the protection of critical national infrastructure (Stettin, 2015).

**International co-operation and mutual assistance**

The proportion of LAC countries implementing international co-operation and mutual legal assistance is low. Only five (Brazil, Chile, Mexico, Peru and the Dominican Republic) are part of the G8 24x7 Contact Network, designed to help national law enforcement authorities in other countries obtain and exchange information related to cross-border criminal investigations, including crime committed through the use of ICTs (Velasco, 2016).

The proportion of LAC countries with mutual legal assistance treaties in the field of extradition and regional judicial co-operation is relatively high. Fifteen countries (Brazil, the Plurinational State of Bolivia, Chile, Colombia, Costa Rica, the Dominican Republic, Ecuador, Guatemala, Honduras, Mexico, Panama, Paraguay, Peru, Uruguay and Venezuela) have extradition treaties and bilateral agreements on international judicial co-operation in criminal matters in force.
**Overall situation**

Several LAC countries have adopted national digital strategies or are in the process of implementing one. Unfortunately, the great majority of national digital strategies in place lack a clear long-term vision on digital security risk and face a number of challenges, such as:

- creating and improving legal frameworks on digital security
- creating operational security risk management capabilities
- a clear distribution of responsibilities among government institutions
- international and multi-stakeholder co-operation (OAS, 2014).

All indications are that the majority of LAC countries are not approaching digital security risk from the economic and social perspective, as called for by the OECD. At the time of writing, this approach is still relatively new, and it is thus not surprising that it is not yet reflected in current policy frameworks. It should also be acknowledged that some LAC countries face various additional challenges that limit their ability to adopt this approach (OAS and Symantec, 2014).

The implementation of co-ordination mechanisms within governments to formulate and carry out national digital security strategies is a key challenge in LAC countries. Instead of distinguishing clearly the various facets of what is often known as “cybersecurity”, and addressing them through an overarching strategy that ensures government co-ordination and coherence, governments often view this issue from a single perspective, such as national security, international security or cybercrime. As a result, the economic aspects are set aside and the issue addressed in isolation from non-governmental stakeholders, in a public policy silo. Budgetary concerns have constrained the adoption of co-ordination mechanisms among government agencies of the region. Only a few countries have allocated annual budgets for national digital strategies by the respective ministries and competent authorities.

Stakeholder engagement in most national digital security strategies has improved, but it is not yet mature in most LAC countries. Many still lack flexible mechanisms and medium and long-term plans to support stakeholders in developing policies and legal frameworks on digital security (OAS and Symantec, 2014). By contrast, a significant number of countries, including Colombia, Mexico, Panama and Peru have established national CSIRTs fully endorsed by their respective national governments, which have been very active in facilitating the exchange of information on security and computer incidents and threats and providing training on information security to their staff and the general public.

The number of LAC countries that have adopted legislation to counter cybercrime pursuant to the Council of Europe’s Budapest Convention keeps growing. Many in the region are interested in formally requesting access to the convention and its Additional Protocol. This, however, will involve a complex and long-term political process.

**Good practices for the LAC region**

**Awareness and understanding of digital security risk management**

Over the years, awareness of digital threats and incidents has increased globally. However, there is still a limited understanding of some aspects and in particular, confusion over its economic and social dimension. The 2015 OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity and its companion document provide key concepts, principles and guidance to develop public policies in this area, as well as policies...
to manage risk in public and private organisations (OECD, 2015a). The OECD approach is based on the recognition that:

- Digital security risk is an economic and social issue rather than solely a technical challenge.
- It is impossible to create a fully safe and secure digital environment where risk is entirely avoided, other than by eliminating digital openness, interconnectedness and dynamism, and thus renouncing any of the associated economic and social benefits.
- Risk can nevertheless be managed and reduced to an acceptable level, determined by the economic and social objectives and benefits at stake, as well as the context.
- Digital security risk management can drive the selection of appropriate digital security measures that do not undermine the activity they aim to protect, take into account the interests of others, and preserve human rights and fundamental values.
- Leaders and decision makers are best placed to steer the changes needed to reduce risk to an acceptable level.
- Digital security risk management should be integrated with economic decision making and the broader risk management framework, to facilitate strategic, agile and effective leadership.

**National Strategy for the Management of Digital Security risk**

Many countries worldwide are adopting what they often call national “cybersecurity strategies”. Their content, however, varies extensively. Regardless of what they are called and the type of document or documents in which they are reflected, it is essential that governments adopt strategies to create the conditions for all stakeholders to manage digital security risk and to increase trust and confidence in the digital environment. Such a strategy may be part of an over-arching policy that addresses the national and international security dimension of cybersecurity, as well as the fight against cybercrime. It can also be included in a national digital strategy to promote the use of ICTs for economic and social prosperity.

Such a strategy should clearly state that it aims 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
- ensure the provision of essential services and the operation of critical infrastructure, protecting 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.

The strategy should 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.

Finally, it should result from a co-ordinated intra-governmental approach and an open and transparent process involving all stakeholders. It should also be regularly reviewed and improved based on experience and best practices, using internationally comparable metrics where available.

The OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (OECD, 2015a) includes guidance for measures that the strategy can include, such as how the government can lead by example, measures to strengthen international co-operation and mutual assistance, how to engage with other stakeholders and how to
create the conditions for all stakeholders to collaborate in the management of digital security risk. Such measures include, for example:

- ensuring that the national digital strategy is conducted and managed in a manner conducive to innovation and prosperity, keeping the environment open, maximising the potential of ICTs for growth and development and facilitating international and regional co-operation
- improving and updating training programmes and ensuring the development of national awareness-raising campaigns
- creating a comprehensive national programme to measure digital security risk and facilitating co-ordination mechanisms and sharing of responsibility among government agencies
- encouraging mutual assistance in the identification of Internet crime and prosecution of perpetrators between law enforcement authorities in the region
- establishing national points of contact to address cross-border requests related to digital security risk management issues and improving responses to domestic and cross-border incidents and threats, including through co-operation with CSIRTs, co-ordinated exercises and other tools for collaboration
- encouraging national partnerships between ICT companies and government agencies on digital security and the creation of flexible cross-border co-operation mechanisms.

**International Cooperation and Mutual Assistance**

International co-operation and mutual assistance is a good policy practice. It can help detect cross-border crime and the development of international and regional co-operation mechanisms to enforce national laws against criminals located in different jurisdictions.

Colombia, Mexico, Peru, Paraguay and Uruguay actively participate in the OAS Cybersecurity Programme and the various activities organised by the Inter-American Committee Against Terrorism (CICTE) to counter cybercrime with the participation of various stakeholders from the public and private sector.

**Engagement with other stakeholders**

Promoting the active participation of stakeholders, through national consultations on digital security, encouraging the management of digital security among different stakeholders, and sharing responsibilities is a good policy practice (Box 14.4).

**Computer Security Incident Response Teams (CSIRTs)**

Computer Security Incident Response Teams (hereinafter CSIRTs) play a key role in identifying threats to information security systems and networks, and crime committed through the use of information technologies. There is consensus that a CSIRT is a “team of experts that responds to computer incidents, coordinates their resolution, notifies its constituents, exchanges information with others and assists constituents with the mitigation of the incident” (Box 14.5). CSIRTs also serve as reliable points of contact for reporting security incidents, disseminating relevant information on computer incidents, mitigating security risks and co-ordinating their response efforts with other similar institutions. Establishing a national CSIRT is a good policy practice to facilitate international and regional co-operation on information security. Private-sector CSIRTs (e.g. business, academia) can also be encouraged.
Box 14.4. Selected cases of national stakeholder participation

Colombia

Colombia expressly considers stakeholder participation in the document “Cybersecurity and Cyberdefense Policy Guidelines”.

Document CONFES 3701, of July 2011, states that the national CSIRT (colCERT) and the CCP will articulate initiatives with the private sector and civil society to manage security incidents for the national critical infrastructure.


Brazil

Brazil’s Internet Steering Committee (Comitê Gestor da Internet no Brasil CGI.br) is a good practice example of multi-stakeholder co-operation that involves the technical community, academia and civil society. In this instance, all share the responsibility for reporting, reviewing and responding to computer security incidents. Responding to threats to networks and systems in the public and private sector and drafting national policies on information security are also part of the task.

Source: Comitê Gestor da Internet no Brasil, www.cgi.br/.

Jamaica

In 2013, Jamaica established a Cybersecurity Taskforce with stakeholders from the public and private sectors that together help to propose, draft and advance national policies on digital security, including Jamaica’s National Cyber Security Strategy.


Box 14.5. Recommendations for the CSIRT community

The Internet Government Forum selected the CSIRTs as one of the topics to be addressed in the Best Practice Forums in 2014. A selection of the recommendations are shown below:

● There is a need for policymakers to discuss the role of CSIRTs with the CSIRT community to avoid misconceptions around the role of CSIRTs.

● CSIRTs are recommended to be actively involved in relevant policy discussion at both the national and international level. In order to engage with other stakeholders it is important to be where they are. The provided examples show that it brings influence and understanding.

● Every government has the right to create the CSIRT it needs. It is recommended though that governments make an informed decision, taking into consideration the potential consequences of their choice.

● Where CSIRTs are concerned privacy and security have to stand together in order for a CSIRT to be truly successful.

● Data protection is a term that is better understood in a general sense than privacy. Hence it is advised to use this term in a CSIRT context more as it is far more concrete.

● Data protection has to be at the core of the work of a CSIRT.

● It is recommended to involve Data Protection Commissioners more in the work of CSIRTs.

● To ensure transparency and accountability where data protection is concerned, it is advised to make a study whether a standard protocol can assist attaining transparency, as well as more conscious decisions about limits to data sharing, anonymisation of data where possible and the handling of data by CSIRTs.
As noted above, 12 countries in the LAC region have a CSIRT fully endorsed or supported by the national government. The cases of Brazil, Costa Rica and Mexico are described here (Box 14.6).

Box 14.6. Selected national CSIRTs

**Brazil**

Brazil has two national CSIRTs in active collaboration. The Center for Security and Incident Computer Networks of the Federal Public Administration (CTIR Gov) is co-ordinated by the Department of Information Security and Communications of the Presidency of Brazil’s Cabinet of Institutional Security. Its main purpose is to monitor and follow-up incidents and threats to computer systems and networks belonging to the Federal Public Administration.\(^1\) Cert.Br is maintained, co-ordinated and sponsored by the Internet Steering Committee (Comitê Gestor da Internet no Brasil CGI.br) and is mainly responsible for the security of information systems and networks of the private and academic sectors, respectively.

1. CTIR Gov is available at [www.ctir.gov.br/](http://www.ctir.gov.br/).

Source: [www.cert.br/](http://www.cert.br/).

**Costa Rica**

Costa Rica created a national CERT (CSIRT-CR) in 2012 as part of the publication of Executive Decree No. 37052-MICT of 9 March 2012. It is composed of the heads of the principal national ministries and is responsible for supporting and co-operating with administrative and judicial authorities to investigate and prosecute cybercrime and co-ordinate activities with Interpol and the OAS’ Inter-American Committee Against Terrorism (CICCTE).

Conclusion

This chapter focused on public policies to increase the management of digital security risk for economic and social prosperity, as distinct from aspects of cybersecurity related to technology, law enforcement, national security and defence. It introduced the key elements of national strategies that can create framework conditions to increase trust for all stakeholders, so that ICTs and the digital environment can be used for economic and social prosperity. These elements include the understanding of risk management as an approach that is focused on the activities that rely on the digital environment, rather than only on the digital environment itself.

The chapter also indicated existing measurement and impact assessment tools and provided an overview of public policy efforts carried out in the LAC region. The general situation in the LAC region is that several countries have adopted national digital strategies or are in the process of implementing one. Unfortunately, the great majority of national digital strategies already adopted lack a clear, overarching long-term vision in relation to digital security risk and face a number of challenges, such as the creation and improvement of legal frameworks on digital security, the creation of operational security risk management capabilities, the clear distribution of responsibilities among government institutions; and international and multi-stakeholder co-operation. All indications are that the majority of LAC countries are not approaching digital security risk from the economic and social perspective as called for by the OECD. However, at the time of writing, this approach is still relatively new, and it is therefore not surprising that it is not yet reflected in current policy frameworks.

Finally, the chapter introduced a number of good practices to encourage digital security risk management policies and strategies, based on the 2015 OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity and its companion document (OECD, 2015a). In particular, policy makers should recognise that digital security risk is an economic and social issue rather than solely a technical challenge. They should also note that it is impossible to create a fully safe and secure digital environment where risk is entirely avoided. As a consequence, they should encourage an approach where leaders and decision makers take responsibility to manage the risk. That means to reduce it to an acceptable level, depending on the context and the economic and social objectives and benefits at stake. All measures in national cybersecurity strategies should reflect this approach, whether they relate to critical information infrastructure, international co-operation or CSIRTs.

Notes


Box 14.6. Selected national CSIRTs (Cont.)

Mexico

The Scientific Division of Mexico’s Federal Police operates a national CSIRT (CERT-MX), currently the official national government CERT. CERT-MX serves as the main point of contact with Interpol and the US Department of Justice. Its activities include the identification and follow-up of computer security incidents, protection of industrial and critical infrastructure and launching national public awareness campaigns on information security.

References


# ANNEX 14.A1

## References to national digital security strategies and national legislation in the LAC region

<table>
<thead>
<tr>
<th>Country</th>
<th>National digital security strategies and national legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dominican Rep.</td>
<td>Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología de la República Dominicana: <a href="http://www.oas.org/juridico/PDFs/">www.oas.org/juridico/PDFs/</a> repdom_ley5307.pdf</td>
</tr>
</tbody>
</table>