Inter-American Development Bank

Institutional Capacity of the State Division (ICS), Institutions for Development (IFD)

TECHNICAL NOTE

No. IDB-TN-588

From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation

Antonio García Zaballos
Félix González Herranz

September 2013

From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation

Antonio García Zaballos
Félix González Herranz

IDB
Inter-American Development Bank
2013

Cataloging-in-Publication data provided by the
Inter-American Development Bank
Felipe Herrera Library

García Zaballos, Antonio.
From cybersecurity to cybercrime: a framework for analysis and implementation / Antonio García Zaballos, Félix González Herranz.
p. cm. (IDB Technical Note; 588)
Includes bibliographical references.
1. Computer crimes. 2. Computer security. 3. Broadband communication systems. I. González Herranz, Félix. II. Inter-American Development Bank. Institutional Capacity of State Division. III. Title. IV. Series.
IDB-TN-588

http://www.iadb.org

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

From Cybersecurity to Cybercrime
A Framework for Analysis and Implementation

Antonio García Zaballos (antoniogar@iadb.org)
Félix González Herranz (felixg@iadb.org)

Abstract

This technical note outlines a framework for the analysis of cybersecurity, presenting considerations that are crucial to the success of a holistic and transversal cybersecurity strategy. It describes two essential pieces of the analysis: the broadband ecosystem and the basic terminology and concepts of cybersecurity systems. These two pieces serve as a basis for the introduction and description of five Priority Action Pillars (PAPs), which represent five clear lines of action that any government should embrace and implement in developing an effective cybersecurity strategy. The five PAPs are complemented by four horizontal recommendations that encompass a comprehensive cybersecurity analysis framework.

JEL Codes: L86, L88, L96, M15, H54
Keywords: Cybersecurity, telecommunications, critical infrastructure, broadband

1. Setting the Groundwork: The Broadband Ecosystem

We are experiencing a new era of communications among human beings through machines. Telecommunications, Internet, and Information and Communication Technologies (ICTs) are transforming our lives and shaping a new panorama of mutual interactions. Exponential technological developments allow citizens, companies, and governments to improve their communication and greatly increase their ability to exchange information.

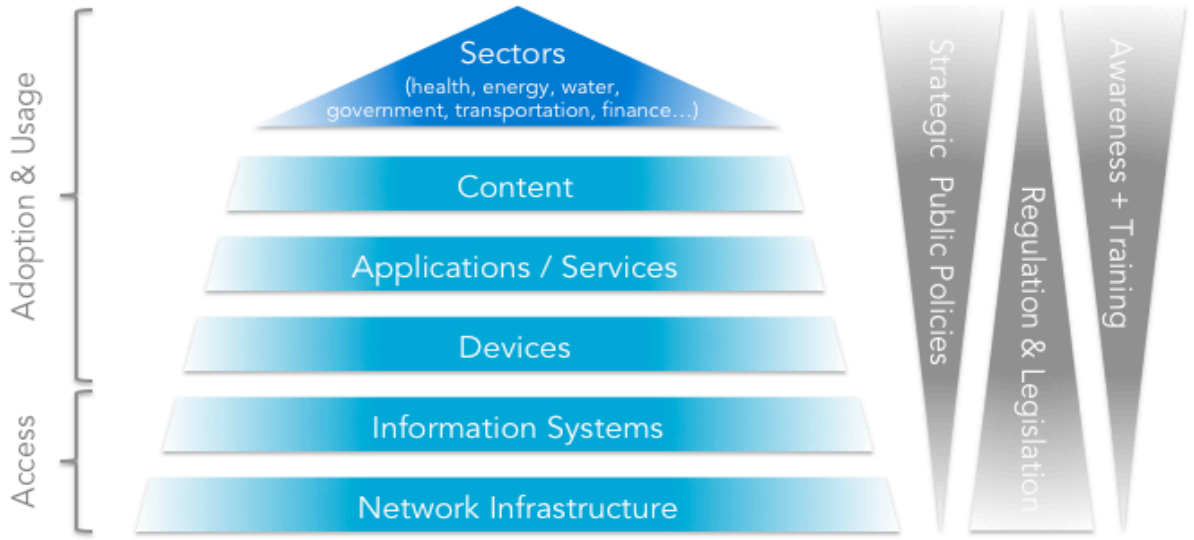
Broadband plays a crucial role as a catalyst for further development of this communication and facilitates economic growth and social inclusion. According to a study published by the Inter-American Development Bank (IDB), in countries where broadband penetration has increased 10 percentage points, there has been an increase of 3.19 percent in GDP, a 2.61 percent increase in productivity, and a net generation of more than 67,000 jobs (García-Zaballos and López-Rivas, 2012).

Despite these facts, it is common to regard broadband as being merely high-speed connectivity and to leave out all of the intertwined social and economic aspects that arise from that connectivity. Broadband is seen more clearly when it is considered, from a holistic perspective, as an ecosystem of pieces that work together to produce outcomes far greater and more complex than simple increases in the speed of data transmission.

The broadband ecosystem can be analyzed from two perspectives. On one hand, it is an *ecosystem of players,* each of whom possesses specific responsibilities and roles. Players include governments, ICT companies, academia, and—the most important players of all—the citizens. On the other hand, there is the vertical perspective: the ecosystem of the pyramid (see Figure 1).

The ecosystem of the pyramid conceives of broadband as a set of supporting layers, ranging from infrastructure to the actual personal use of those connectivity elements. Nonetheless, the layers should not be seen as additive, but rather as part of a comprehensive ecosystem that must be considered as a whole. For instance, content on the Internet is only accessible and relevant when there is an application that carries it, a device that allows use of the application, managing information systems, and an efficient network infrastructure. Infrastructure would be a dump channel without all of these layers put together. Moreover, the different players fill a key role in each of the elements in the ecosystem of the pyramid.

Figure 1: The Ecosystem of the Pyramid



1.1. Key Elements

The approach considers the different elements on the supply side (access) as well as on the demand side of the equation (adoption and usage). It is important to note that the ultimate goal is to support the development and the transformation of each of the sectors of the economy; this is what happens with a user-centric approach, which guarantees that all efforts are for the benefit of the citizens.

1.1.1. Access Elements (Supply)

Access elements comprise network infrastructure and information systems that support the whole ecosystem, because they enable applications, information, and knowledge to be exchanged. Network infrastructure refers to pure telecommunications infrastructure (i.e., the network), the composition of which depends upon the different technology alternatives available in the market and those actually deployed on the ground. Information systems, on the other hand, are constructed from a wide spectrum of options, ranging from databases and data warehouses to servers and dedicated computers. These components are located in either private or public facilities.

1.1.2. Adoption and Usage Elements (Demand)

Adoption and usage elements are closer to the user and, thus, more familiar to all of us. There is a wide variety of devices, such as personal computers, laptops, tablets, smartphones, and other gadgets. These devices are now able to connect to the Internet via the machine-to-machine (M2M) technologies embedded in cars, trucks, streetlights, and so forth. However, in many countries, these devices are actually a bottleneck that impedes the creation of content and keeps broadband from being expanded (i.e., demand is not generated). This fact requires governments to create and implement new public policies that boost broadband usage, which must be coupled with training in how to use broadband and ICTs.

The device panorama is boundless and changes rapidly along with the applications that run on the devices. Applications range from simple weather forecasts on smartphones to more complex applications, such as fleet control systems. These applications support the piece of the ecosystem that matters most to users—the content. In addition to supporting the content by acting as a means of delivery, the applications are often the means by which new content is created.

These horizontal elements support the different sectors of the economy and the citizens themselves. However, it is important to note that, even though the network infrastructure and information systems (the latter requiring a certain degree of customization per sector) are completely transversal to all of the sectors, the rest of the elements (devices, applications, and content) depend largely on the specific type of sector (e.g., an e-banking application is largely different from an online education platform).

1.1.3. Supportive Elements

The ecosystem of the pyramid considers three vertical elements that are essential for the entire ecosystem: awareness and training, regulation and legislation, and public policies. These three components foster the development of the different horizontal elements.

Most people are well aware of the Internet, ICTs, and broadband. However, there are still some who lack access to them (due to a lack of infrastructure and/or devices and broadband services that are prohibitively expensive) or, even though they have access, they are not aware of the benefits that the technology brings. For that reason, it is crucial to create awareness programs to inform citizens, companies (with a particular focus on small and medium enterprises), and public administrations of the benefits and how to gain access to the Internet and ICTs. Moreover, these activities need to be coupled with training and capacity building programs to make it easier for people to learn and take advantage of the new technology. It is worthwhile to note that the efforts should be leveraged at the upper part of the ecosystem (e.g., health, education, financial inclusion, etc.) in order to directly benefit the greatest number of people. Technical skills are crucial at the infrastructure level, but those skills are more specific and, thus, more easily taught on a smaller, institutional basis. The Ministry of Education in each country needs to take action to ensure that pathways to technical degrees and specializations are available to all citizens.

Regulation and legislation provide the basis for a thriving ecosystem by fostering competition and facilitating investment. For this reason, these factors are more relevant to the bottom of the pyramid, where they act to stimulate higher levels of capital investment. Nonetheless, it is important to bear in mind the dynamism in the field of application development and technology in general, which requires up-to-date legislation that is capable of protecting business and users in matters such as transactions, privacy, confidentiality, and digital identity.

Finally, public policies are the specific strategies that boost the development of each of the layers. More importantly, on the demand side, they should favor the adoption and usage of technologies to guarantee the universality and affordability of access to ICTs and broadband. Examples of supply side policies are infrastructure-sharing strategies and the well-known holistic national broadband plans. On the demand side, there are subsidies, tax reductions on ICT services, and training programs.

2. Defining the Cornerstone Concept of Cybersecurity

The elements of the broadband ecosystem and the use of the Internet are defining a new concept in the ICT arena called *cyberspace,* which is the digital realm in which people, companies, governments, and machines communicate with each other and carry out transactions. This communication requires two common nexuses: (i) network connectivity and (ii) the exchange of information by means of remote access, which plays a key role in facilitating the externalities of the transactions. As in other sectors, these transactions can result in negative externalities. Specific examples include information robbery, *cyberattacks,* and *cyberespionage*.

In this new environment of digital interactions and transactions, cybersecurity is of critical importance, particularly when it comes to: (i) preventing and identifying the vulnerabilities of the network environment in which transactions take place; (ii) analyzing the likelihood and potential harm of *cyberthreats*; (iii) assessing the consequences if the threats become real attacks; (iv) estimating the direct and indirect costs and impact of the *cyberattack*; (v) assessing the costs of potential countermeasures; and, finally, (vi) selecting the appropriate security measures, possibly using a cost-benefit analysis (World Economic Forum, 2008).

2.1. Defining the Cyber Basics

There are multiple concepts associated with the word *cyber*. The challenge today is to clearly understand what these concepts represent and, therefore, manage a common and unified vocabulary when talking about cybersecurity issues. At the same time, it is true that the meaning of some of the concepts overlap and the concepts are often misplaced. The following list provides some important definitions (UN-ESCAP, UN-APCICT, and Ministry of Strategy and Finance, Republic of Korea, 2008):

- Cyber vulnerability is susceptibility in the protection of an asset from cyberthreats.
- Cyber risks are the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.
- Cyberthreats are potential cyber events that may cause unwanted outcomes, resulting in harm to a system or organization. Threats may originate externally or internally and may originate from individuals or organizations.
- Cyberattacks are the use of malicious codes that may affect computers and networks, and lead to cybercrime, such as information and identity theft.
- Cybersecurity encompasses all the necessary elements required to defend and respond to cyberthreats in cyberspace (e.g., technology, tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, and assurance, among others).
- Cyber resilience is the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery.

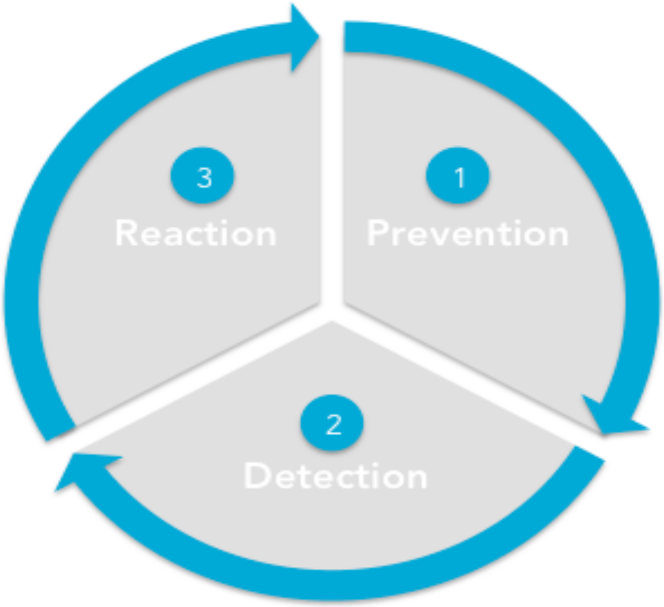
- Cybercrime refers to the different forms of crime that involve computers or networks when they are used to attack or are attacked.

2.2. The Cybersecurity Cycle

Due to the extension of potential harm across time, any cybersecurity strategy must be grounded on the cybersecurity cycle, which includes the following three stages (UN-ESCAP, UN-APCICT, and Ministry of Strategy and Finance, Republic of Korea, 2008):

1. **Preparedness and prevention**: relates to preparing human users and machines to protect themselves against any cyberthreat, while promoting security and the avoidance of particularly vulnerable technologies.
2. **Detection:** refers to identifying threats as quickly as possible.
3. **Reaction**: relates to recognizing and correcting the causes of a disruption.

Figure 2: The Cybersecurity Cycle



Source: Authors' elaboration.

3. Cybersecurity in the Ecosystem

When discussing cybersecurity, it is important to consider the two dimensions of the ecosystem: the players (the ecosystem of players) and the elements (the ecosystem of the pyramid). Cybersecurity is the glue that holds all of the players together at all levels of the ecosystem. Moreover, it is important to advocate for including cybersecurity measures in any ICT endeavor, either at the level of a national broadband plan or as part of a national digital agenda.

3.1. The Implication of Cybersecurity in the Ecosystem

As for the ecosystem of players, the challenge and necessity are to involve all of the players in the cybersecurity discussions, and to capture their commitment when making agreements and taking actions in cyberspace. It is important to understand that if one element of the ecosystem fails, the harm can affect the rest of the players. This also includes the end users, who are often the source of vulnerabilities and the target of cyberattacks, due to their lack of knowledge or risky online behavior. This fact suggests two crucial actions. First, it is necessary to create awareness of the importance of cybersecurity for citizens, companies, governments, and academia. Second it is important to train users, both at a technical and nontechnical level, in order to protect the most vulnerable group of users from cyberthreats, as well as to defend the ecosystem from the risky online behavior of those same users.

This leads to the second dimension of the ecosystem: the ecosystem of the pyramid. All of the layers, along with the policies, regulations and legislation, and awareness and training (i.e., capacity building) must include a component of cybersecurity. Specific actions and strategies are necessary to protect the critical infrastructure (including the infrastructure and the devices in the ecosystem of the pyramid) and the critical information (including applications and content in the ecosystem of the pyramid) from any unauthorized access, modification, theft, disruption, or interruption. These actions and strategies are the following:

- Networks and information systems need to be equipped with preventive, detective, and reactive elements. Some of these are autonomous, and some are tools used by people to perform the necessary actions throughout the cybersecurity cycle. In this sense, hardware manufacturers need to design their products with physical elements that protect against vulnerabilities and with software that detects threats and repels attacks.

- Devices are the most common entry point for cyberattacks, because they are directly used by people who, in most cases, are unaware of the threats. Although the people managing the network and information systems are highly technical and conscious of the importance of cybersecurity, sometimes, the device is subject to an attack or receives malicious code, and the user is not aware of it until something negative happens (e.g., identity theft or the impairment of the performance of the device). Traditionally, personal computers and laptops were most vulnerable to exploitation by viruses, Trojan horses, and the like. However, due to the explosion of the smartphone market, the focus of cybercriminals is gradually shifting toward these devices. Fortunately, most devices have specific hardware elements that protect them against certain threats; however, the greatest protection comes from the next layer: the applications.
- In terms of cybersecurity, the most well-known applications are antivirus software programs. These exist as an additional source of protection, especially in the prevention phase. Moreover, there is a wide range of other applications, particularly for smartphones, that increase security and protection. In that space, software developers play an important role in creating applications that are capable of detecting potentially harmful software and helping the user reject malicious code.
- The last element is that of content, which is often the source of cyberattacks. Users are often deceived by malicious code, which is used to gather information from the user, such as usernames, passwords, and credit card details (e.g., phishing). Preventive actions around content and training for users on the topic of the safety of content are crucial elements of a comprehensive cyber security strategy.

It is important that cybersecurity be in place across the horizontal elements of the ecosystem of the pyramid, as well as in all of the vertical elements. It is crucial to create awareness of the importance of cybersecurity, such as through mass training efforts for all citizens (school, work, and government) and dissemination campaigns, as was the case for ICT and broadband services. Regulation and, more importantly, legislation are essential to provide a strong and robust cybercrime framework that deters criminals from carrying out their attacks.

As for public policies (some of which were mentioned previously), the government needs to take the lead, coordinating role to ensure that the policies are embraced by all of the stakeholders (i.e., the ecosystem of players). An illustrative example is the creation of a national Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT), which operate across the three phases of the cybersecurity cycle. (More than one team may be needed, depending on the needs and the amount of *cybertraffic* in a country.) Other examples are the pure regulation and laws aimed at deterring people from committing crimes (prevention) and prosecuting them when they do commit crimes (reaction).

Another important aspect is the security of critical infrastructure, which are the elements connected to cyberspace that are crucial for the successful functioning of the different sectors of the economy. These components, which are also potential targets of cyberattacks, can be found both within and outside of the telecommunications networks, such as medical record information systems, energy grids, airport traffic control, transportation systems, gas pipeline networks, and so forth. If they were compromised, it could lead to service disruptions or, in the case of a terrorist attack, more serious consequences.

3.2. Important Steps to Ensure Cybersecurity

Cybersecurity is not only a framework or a set of on-time actions, but it is also a set of ongoing efforts focused on performing periodic assessments and monitoring of the aforementioned policies, as well as enforcing compliance with existing regulations and laws and applying sanctions in the case of violations. According to the International Telecommunications Union (ITU, 2008), from the public sector point of view, there are clear steps that any government needs to take to ensure the success of a cybersecurity strategy (see Table 1).

Table 1. Key Aspects for a Successful Cybersecurity Strategy

1	Persuade national government leaders of the need to develop policies that address threats and vulnerabilities on the national cyberinfrastructure and information (this includes the digital identity of humans, institutions, and machines). It is also very important to define the governance model for the cybersecurity strategy and to clarify how the different roles and responsibilities are distributed among the entities involved.
2	Identify a person and an institution to lead the overall national effort. That person and that institution are entitled to direct and coordinate the efforts of governmental institutions, while guaranteeing that they can effectively interact with the private sector.
3	Identify the appropriate experts and policymakers within government agencies and the private sector and determine how to involve them in developing and implementing the different parts of the national cybersecurity strategy.
4	Identify cooperative arrangements for and among all participants in formal and informal ways so that information sharing is encouraged between public and private sectors during the entire cybersecurity cycle.
5	Identify international counterparts and coordinate efforts to address cybersecurity issues, including sharing information and best practices.
6	Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity.
7	Periodically assess the state of cybersecurity efforts and develop and adjust program priorities.
8	Identify training requirements and create a training plan.

Source: ITU (2008).

4. Cybercrime as a Consequence of a Failing Cybersecurity Strategy

Cybercrime is known by different names, such as computer crime, e-crime, and electronic crime. All of these terms refer to crimes in which computers or networks are used to perform attacks, or when networks themselves are attacked. Obviously, cybercrime happens every time cybersecurity is breeched. For that reason, cybercrime is seen as a consequence of a failure of cybersecurity. The efforts encompassed by a holistic cybersecurity strategy should consider how to best address cybercrime and enforce the associated regulations and laws. The Convention on Cybercrime identified four different types of offences: offences against the confidentiality, integrity, and availability of computer data and systems; content-related offences; copyright-related offences; and computer-related offences.[1]

In order to address cybercrime, it is necessary to establish effective laws and regulations through the following steps:

- Assess the current legal authorities and framework for adequacy. Countries should review existing criminal code and include procedures to address current (and future) problems.
- Draft and adopt substantive, procedural, and mutual assistance laws and policies to address cybercrime.
- Establish or identify national cybercrime units.
- Develop cooperative relationships with other actors involved in the national cybersecurity infrastructure, in both the public and private sector.
- Develop an understanding among prosecutors, judges, and legislators that deal with cybercrime issues.
- Participate in the 24/7 Cybercrime Point of Contact Network.[2]

5. The Five Priority Action Pillars (PAPs)

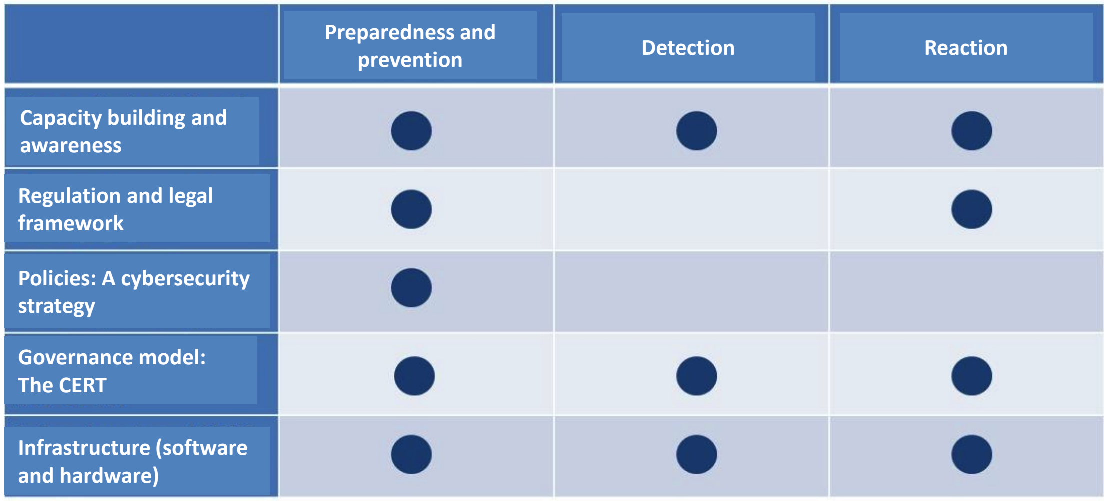
A holistic cyber security plan should include five PAPs that simultaneously address the different phases of the cybersecurity cycle (see Figure 3). The proposed pillars summarize many of the concepts that were explained previously. They are obviously incremental and complementary in effect, but it is important to consider each pillar to have the complete view of the cybersecurity plan and the degree to which it meets its objectives. For instance, it is useless to maintain a robust infrastructure without a well-trained CERT that is able to manage the attacks and implement the responses. Investments in infrastructure and a CERT would be ineffective if the country lacks the regulatory and legal mechanisms necessary to address cybercrime. The pillars are prioritized depending on the degree to which cyber security is developed in the specific country. Additional pillars can be put in place, such as policies that foster the creation of cyber innovation (e.g., protective software) within the country.

[1] The Convention on Cybercrime, the first international treaty addressing cybercrime, was entered into force in July 2004. See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[2] This is a network of emergency cybercrime contacts that was established to improve international assistance in urgent investigations that involve electronic evidence.

In this regard, the ultimate goal is the protection of the critical infrastructure and information of the country. To achieve this goal, it is important to consider three strategic objectives that coincide with the cybersecurity cycle: (i) prevent cyberattacks, (ii) reduce national vulnerabilities to cyberattacks, and (iii) minimize damage and recovery time from cyberattacks.

Figure 3. The Cybersecurity PAPs and Cycle



	Preparedness and prevention	Detection	Reaction
Capacity building and awareness	●	●	●
Regulation and legal framework	●		●
Policies: A cybersecurity strategy	●		
Governance model: The CERT	●	●	●
Infrastructure (software and hardware)	●	●	●

Source: Authors' elaboration.

5.1. Pillar 1: Capacity Building and Awareness

This topic was extensively described in Section 3.1. The objective of this pillar is to work around two axes: (i) to create awareness of the importance of cybersecurity at all levels across public and private actors and citizens and (ii) to develop comprehensive training programs on the subject. The trainings are delivered in both technical and nontechnical formats. Technical training (incorporating cybersecurity and cybercrime) is provided at universities, law schools, and technical colleges. Nontechnical training (in the three steps of the cybersecurity cycle: prevention, detection, and reaction) is provided to all citizens, most of who are end users.

5.2. Pillar 2: Regulation and Legal Framework

It is clear that regulation and legislation are crucial to foster a *cyber environment* that contains the mechanisms necessary to successfully fight cybercrime. Three points stand out as crucial to forming an effective regulatory and legal framework. First, regulations and laws must be modern, updated, and robust. The ever-changing specifics of cybercrime require the constant update of laws and regulations. A lack of vigilance in this area favors the appearance of the aforementioned cybercrime havens.

Second, and also related to the former point, it is important to maintain dynamic frameworks; in other words, to update them according to the new shapes that cybercrime and cyberterrorism may take. Cyberterrorists stay one step ahead of the authorities and always seek new methods of attack. Regulations and laws need to be modern and flexible enough to meet the challenges and, when possible, anticipate them and act accordingly. In addition to the obvious effect of facilitating the investigation and prosecution of crimes, strong legislation signals to cyberterrorists that the country possesses a robust police and criminal justice system, which may deter them from committing crimes in that country.

Finally, although a challenging task, it is crucial to foster regional coordination and harmonization in order to establish common regulatory and legal frameworks so that some countries do not become cybercrime havens. The process is already under way in some regions (e.g., the European Union).

5.3. Pillar 3: A Cybersecurity Strategy

A cybersecurity strategy is the cornerstone of all the actions that a country as a whole may conduct in the cybersecurity arena. Its ownership needs to remain within the national government, because it manages the efforts of the country as a whole. Nonetheless, due to the nature of this topic, a successful cybersecurity strategy requires a coordinated effort among all the stakeholders involved, including the public sector, private sector, citizens, nongovernmental organizations (NGOs), academia, and so forth.

Moreover, an effective strategy must incorporate all five PAPs to cover the landscape. At the same time, it must take into account the full cybersecurity cycle and define specific actions for each of the three phases. Although the cybersecurity strategy tends to linger in the prevention phase because it contains actions and plans that need to be completed before moving forward, it is also true that its effect and impact touch upon the detection and reaction phases as well.

The last important point to keep in mind regarding this strategy is the governance model (as is true for any strategy). In addition to actions and plans, the strategy must identify the specific stakeholders involved and their responsibilities, and determine the most effective mechanisms of coordination and information sharing.

5.4. Pillar 4: Governance Model: the CERT

The protection of a whole country begins with having a central agency that coordinates the efforts of the institutions and serves as an interface with the international community. Both the National Computer Emergency Response Team (CERT) and the Computer Security Incident Response Team (CSIRT) play this role. These agencies intervene across the three phases of the cybersecurity cycle: prevention, detection, and reaction.

It is worth noting that a country may need multiple CSIRTs (or CERTs), due to the amount of network traffic volume and the number of cyberincidents that occur. This may require an additional level of coordination: it is important that only one of the CSIRTs holds ownership of the overall coordination of the teams, whereas the rest of the CSIRTs fulfill their specific responsibilities and mandates within their areas of expertise or working knowledge (e.g., there are CSIRTs for financial services, government services, universities, companies, regions, etc.). In any case, it is the responsibility of the government to promote the creation and development of the coordinating CSIRT and to place it within the correct government structure. Some governments may decide to place it within the ICT or the Telecommunications Ministry (e.g., Panama), while others place it within the Ministry of Defense (e.g., Ecuador). Others may identify a different suitable place.

For all of these reasons, the CERT (or CSIRT) needs to be empowered as the main coordinator not only for technical actions, but also for strategic actions such as implementing training plans and defining coordination plans. It is also important to guarantee its independence and impartiality so that all stakeholders trust their work and are able to provide the necessary information when an attack or vulnerability is detected. Due to its technical nature, the CERT is composed mainly of technical personnel that communicate effectively with their counterparts in other institutions.

5.5. Pillar 5: Critical Infrastructure (Software and Hardware)

As explained in Section 3.1, cybersecurity involves both hardware (networks and information systems) and software elements (applications). Any hardware or software element can be the vulnerable to an attack (i.e., *cybervulnerable*). However, certain elements constitute the critical infrastructure and require special attention, because if they suffer an attack, the consequences can be tremendous (e.g., the disruption of telecommunications networks, transportation systems, airports, and so forth).

The strategic actions related to critical infrastructure begin with building an infrastructure map that identifies all of the critical elements. It is important to bear in mind that the critical infrastructure components do not necessarily have to be managed by public agencies. There are many infrastructure components that are part of private companies, such as the computer servers of a bank or private hospital. For that reason, the coordination with all of the stakeholders is, again, crucial.

Once the critical infrastructure is identified, it is necessary to define a specific action plan for those elements across the cybersecurity cycle of prevention, detection, and reaction. It is important that the plan is customized to the specific element. Some components of the plan may be common to all of the elements, but there are specific actions or strategies intrinsic to each element. For instance, the reaction to an attack on the control system of an airport differs from the reaction to an attack on the server holding the health records of a hospital, especially in terms of reaction time and resources allocated to combat the attack.

5.6. The “AS-IS” and “TO-BE” Exercise

To maximize the potential of the five pillars, it is important to first perform an assessment of the status quo of the security environment, and then define the ideal situation. To identify the gaps that need to be filled between the two, it is important to complement the assessment with an analysis of best practices in other parts of the world. Inputs from other relevant players in academia and the private sector must also be included. Once the assessment is finalized, specific plans and actions can be developed and implemented with the aim of bridging the gap between the current and desired status. It is important to bear in mind that the plans must include a strong technical as well as financial component.

6. Final Recommendations

The five PAPs offer the comprehensive strategic framework needed to carry out actions in the cybersecurity arena that positively impact the whole ecosystem. To increase the likelihood of success, all players involved in executing the strategy should follow these final recommendations, which perfectly complement the five PAPS:

1. *Grant maximum visibility to cybersecurity at a national level*. The reasons for this are twofold. First, cybersecurity is necessary to guarantee the security of the country, which has great implications for the health of the economy and the political system. Second, if actions are sponsored by the nation from the highest levels of government, the likelihood of the proper implementation of programs, plans, and agendas greatly increases. Effective implementation encourages the stakeholders to stay involved, which, in the case of cybersecurity, is challenging but crucial, due to the importance of maintaining a holistic and multi-stakeholder approach that ensures definition and implementation of a robust strategy.
2. *Government, private, and academic (GPA) sector collaboration and information sharing.* These are crucial for carrying out coordinated actions and learning about threats. It is important to remember that cyberspace changes rapidly, and cyberthreats and vulnerabilities appear and develop at a faster pace than the advances in the detection and prevention systems. For this reason, stakeholders must have a trusted environment where they can share information about current attacks or threats. This environment allows for more effective and timely reactions. It also requires a single point of coordination, such as the CSIRT, and consolidation of the information that guarantees confidentiality and is capable of triggering the necessary actions. Collaboration and information sharing within and between countries are essential to avoid the creation of cybercrime havens.
3. *Confidentiality.* As mentioned, confidentially is crucial when dealing with cyberattacks and vulnerabilities, as it guarantees a safe and trusted environment in which private companies and public institutions are willing to share their cybersecurity information and best practices. As one can imagine, a leak of this information can have disastrous effects on the reputation and success of an organization.

4. *Assessment and implementation* are two consecutive steps. As mentioned, it is necessary to conduct a deep assessment of cybersecurity on a national and regional basis in order to gain a thorough knowledge of the current status of cybersecurity and cybercrime. The assessment must be followed by the definition of a cybersecurity strategy that contains all of the regulatory and legal implications. The most important aspect is to ensure that all stakeholders implement the strategy, so that coordinated and effective actions are put in place. Likewise, a monitoring program should be implemented for the purpose of conducting ongoing assessments and implementing changes and specific actions as needed over time.

References

García-Zaballos, A. and R. López-Rivas. 2012. "Socioeconomic Impact of Broadband in Latin American and Caribbean Countries." Technical Note No. IDB-TN-471. Washington, DC: Inter-American Development Bank. Available at http://www.iadb.org/en/publications/publication-detail,7101.html?id=62086.

International Telecommunication Union (ITU) Study Group Q.22/1. 2008. "Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts." ITU-D Secretariat Draft. January 2008. Geneva, Switzerland: ITU. Available at http://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf.

Organization of American States and Trend Micro. 2013. "Latin American and Caribbean Cybersecurity Trends and Government Responses." Washington, DC: Organization of American States. Available at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.

United Nations Economic and Social Commission for Asia and the Pacific (UN-ESCAP)/Asian and Pacific Training Center for Information and Communication Technology for Development (UN-APCICT) and Ministry of Strategy and Finance, Republic of Korea. 2012. "Knowledge Sharing Series. Issue II. Cybersecurity." Republic of Korea: UN-APCICT/ESCAP. Available at http://www.unapcict.org/ecohub/Cybersecurity_190312.pdf

World Economic Forum. 2012. "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience." Geneva, Switzerland: World Economic Forum. Available at http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

Annex 1. About the Authors

Antonio García Zaballos is a lead specialist on telecommunications in the Institutional Capacity of the State Division of the Inter-American Development Bank, where he heads the Broadband Program, which includes all cybersecurity matters. He has more than 14 years of experience in the telecom sector, where he has worked in different positions and companies. At Deloitte Spain, he led the practice of regulation and strategy. He was also the head of the cabinet for Economic Studies of Regulation at Telefónica of Spain and the deputy director of economic analysis and markets at the Spanish Telecom Regulator (CMT). He holds a PhD in economics from the University of Carlos III in Madrid, Spain, and is an associate professor of applied finance in telecommunications at the Instituto de Empresa Business School. He is the author of several publications on economic and regulatory matters for the telecommunications sector.

Felix González Herranz is a telecommunications consultant in the Institutional Capacity of the State Division of the Inter-American Development Bank, where he is the technical and strategic lead of the Broadband Program, which includes all cybersecurity matters. He has more than four years of experience in the telecom sector where he has worked in different domains and countries at institutions such as the World Bank, France Telecom, Telefonica, and Capgemini. He is also a social entrepreneur who launched a philanthropic initiative, Juntosalimos, in Spain, his home country, and volunteered as a mentor at Stanford University. Felix holds bachelor's degrees in electrical engineering and in computer science from Universidad Politecnica de Madrid (Spain) and TELECOM ParisTech (France), respectively, and a master's degree in management of science and engineering from Stanford University, where he studied on a Fulbright scholarship.