Volume 2, November 2016

Global Cyber Expertise Magazine

Mauritius Cybersecurity Strategy
A Tool for Better
Cyber Protection
-page 7-

"Pokémon Go"
Legal Implications
in Brazil
-page 16-

Interview with Lynn St. Amour
Chair, IGF Multi-stakeholder
Advisory Group
-page 32-

Cyber security guide for business

Five principles to identify risks, six key actions companies should take
-page 26-

AFRICAN UNION

GFCE
Global Forum on Cyber Expertise

OAS More rights for more people

Volume 2, November 2016

Global Cyber Expertise Magazine

Editorial

Regions

Africa

America's

Asia & Pacific

Europe

Global developments

Editorial

Welcome to the second edition of the Global Cyber Expertise Magazine! Jointly published by the European Union, the African Union, the Organization of American States and the Global Forum on Cyber Expertise, this magazine allows policymakers to stay abreast of current developments on global capacity building projects and policies related to cybersecurity.

This second issue provides a well-rounded overview of the current status of cybersecurity throughout the globe, including the risks, challenges and opportunities that some countries encounter. As the use and development of ICTs grows, so does the risk of cyber related crimes, threats and attacks. Our article on West Africa examines the fight against cybercrime in the region, explaining the challenges associated with limited human resources, as well as the need for effective legal and regulatory frameworks. On a similar note, our case study on Mauritius examines the potential benefits of implementing a Cybersecurity Strategy and how this can improve a country's response to cyberattacks. With regards to Latin America, the author explores how Information Security Risk Management can help increase the cybersecurity mindset of governments throughout the region. And in Australia, we illustrate the possibility of advancing and protecting the country's interests online in an age where the government needs to expand its cybersecurity capabilities, respond to cyber threats and promote norms and behaviors that are consistent with a secure, free and open Internet.

This issue also highlights some innovative experiences in the global quest to improve cyber security capabilities, such as the 2016 Meridian Conference, which focused on developing capacities in Critical Information Infrastructure Protection (CIIP), as well as the 2016 GFCE Annual Meeting that gathered over 100 cyber policy makers and stakeholders from throughout the world to exchange experiences on cybersecurity capacity building initiatives.

The "Cyber Security Guide for Business" developed by the International Chamber of Commerce (ICC), identifies 6 security actions you can take to address cyber security challenges and raise awareness for online security in your business. And finally, the case study on the legal implications of "Pokémon Go" in Brazil provides an interesting view on the risks associated with new online games and the increased availability of personal and sensitive data on the internet.

As we work to develop the next issue of this magazine, we invite you to share information regarding cybersecurity conferences, workshops, training events, policies or case studies that other global entities might find useful. We would be particularly interested to learn about new capacity building initiatives, legislations or strategies in cybersecurity.

We hope you enjoy this issue of the Global Cyber Expertise Magazine and look forward to your continued feedback.

Alison August Treppel

Cybersecurity and the fight against cybercrimes in West Africa: current status, challenges and the future

The growth in the use and development of information and communications technologies (ICTs) go hand in hand with the rise of cyber related crimes and activities in West Africa. This makes for interesting times in the region, as measures need to be put in place to ensure that ICT growth is not stifled and cybercrimes are curbed. A number of cyber related Supplementary Acts to support the secure use of ICT services have been adopted within the Economic Community of West African States (ECOWAS) and are currently under implementation by Member States. In addition, the ECOWAS, in collaboration with various partners, is working to ensure the secure use of ICT services among its Member States.

Written by: Folake Olagunju Oyelola, Program Officer - ICT, Internet & Cybersecurity Policy, Telecommunications Directorate of the ECOWAS Commission.

The Economic Community of West African States (ECOWAS) is a regional organisation of 15 Member States with a mandate to promote economic integration in all fields of activity of its constituent countries. Information and communications technologies (ICTs) play a key role in this context, given the fact that the ICT service sector is an important component of all ECOWAS Member States' economies. The ubiquitous nature of the use of ICTs provides West Africa, a region of over 300 million people and counting, with unprecedented opportunities to accelerate social and economic development. Nevertheless, the misuse of ICTs and their vulnerabilities create cybersecurity and cybercrime issues.

Current Status and Challenges

The myth that only the Global North deals with cybersecurity and cybercrime issues can be dispelled, as today West Africa is more interconnected than ever before and the reliance of ECOWAS countries on the

Cybercrime Capacity Building Workshop

> **“West Africa is more interconnected than ever before and the reliance of ECOWAS countries on the internet is on the increase”**

internet is on the increase, with an equal rise in the region’s vulnerability to cyber threats. For instance, the Minister of Communications for the Government of Nigeria announced a yearly loss of around 127 billion naira, due to cybercrime activities.

The region can be deemed an environment conducive to cybercrime activities for a number of reasons, such as:

a. Inadequate implementation of adopted legal and regulatory frameworks at the national level;
b. Sophistication of cyber-attacks and Governments' limited capacity to deal with the complexity of cybercrime issues;
c. Limited technical and legal human capacity/expertise; and
d. Lack of awareness campaigns to sensitise stakeholders on cybersecurity and cyber laws.

With this in mind and in order to protect the citizens and businesses of West Africa, two supplementary acts on Electronic Transactions and Personal Data Protection were adopted in 2010, as well as a Directive on the Fight against Cybercrime within ECOWAS in 2011.

- The Supplementary Act on **electronic transactions** recognises the existence of such transactions in the ECOWAS space and defines the rules to regulate these activities, notably the obligations and responsibilities of actors, as well as measures to secure electronic transactions;
- The Supplementary Act on **personal data protection** aims to fill the legal gap relating to personal data protection within the Community. It is also aimed at establishing in each ECOWAS Member State, a mechanism to protect privacy through personal data collection, processing, transmission, storage and use; and
- The Directive **on fighting cybercrime** is aimed at bridging the legal gap related to cybercrime repression through the adoption of new offences specific to ICT. It also aims at adapting traditional offences related to ICT offences, sanctions and the punishment regime in force in Member States, to the new technological environment.

These community acts are being implemented by Member States in varying stages. The challenges faced by Member States include:

a. Lack of critical mass of expertise (Police, IT, Judiciary)
b. Only a few Member States have set up a Computer Emergency Response Teams (CERT)
c. Inadequate cooperation between Member States and the global community on cybercrime (investigation, electronic evidence etc.)

"A collective approach and responsibility is required to minimise the impact cybercrimes have on the region"

Cybercrime Capacity Building Workshop

Moving forward

The borderless nature of cybercrime remains particularly challenging for ECOWAS countries. To achieve cybersecurity within the region, ECOWAS Commission developed a cybersecurity agenda in 2015 - "Enhancing Cybersecurity in ECOWAS region" to support Member States in strengthening their cybersecurity capabilities, to respond better to cyber threats and to ensure enhanced protection of their national infrastructure, thereby making the Internet safer and protect Internet users.

To move forward, the region also requires a combination of legal instruments, targeted awareness and sensitisation campaigns, as well as more capacity building workshops that cut across Member States' Governments, highlighting the impact cybercrimes can have on countries' socio-economic development. Various capacity building exercises have been conducted with a number of partners both on technical and legal issues, namely Global Forum on Cyber Expertise (GFCE), Council of Europe (CoE), Cybersecurity Alliance for Mutual Progress (CAMP), United Nations Conference on Trade and Development (UNCTAD) and the United States Government. Nonetheless, more capacity building initiatives are needed to develop technical and human expertise in the region.

As the threat of cybercrime remains omnipresent, Member States need to understand that a collective approach and responsibility is required to minimise the impact cybercrimes have on the region. To this end, ECOWAS has established various ongoing partnerships with GFCE, CoE, CAMP, ITU, among others, to encourage more public-private strategies to promote cybersecurity, as well as to enhance regional cooperation. Cybersecurity is a shared responsibility, and only by sharing information and best practices with different partners will the West African region be able to move forward in the fight against cybercrime.

Cybersecurity Strategy: A Tool for Better Cyber Protection

The rapid growth of the Internet population has contributed to the economy and provided new opportunities to many African countries. But the rising cyberspace has also created significant challenges by opening up new threats. The absence of adequate measures in many African countries makes them more prone to cyber-attacks. One of the key instruments for providing a response to cyber-attacks is to have an effective cybersecurity strategy which acts as a shield for a variety of attacks. This article describes the ground realities of developing and implementing the cybersecurity strategy in Mauritius and outlines the main ingredients of the strategy document.

Written by: Dr. Kaleem Ahmed Usmani and Mrs. Jennita Rao Appanah, Computer Emergency Response Team of Mauritius (CERT-MU), National Computer Board, Mauritius

Introduction

The Internet and digital technologies are transforming African nations, in part by acting as drivers for economic growth and by providing new ways for communication and cooperation. While this change acts as a catalyst for boosting the countries' efficiency and productivity, it also creates a number of challenges in maintaining users' trust and confidence in the cyber environment. With the emergence of new threats to the online environment, the cybersecurity landscape has changed massively. In the face of increasing cyber threats and the sophisticated nature of cyber-attacks, African nations require a cohesive and comprehensive national cybersecurity strategy to be developed and implemented to respond effectively. This will help in creating a secure and reliable online environment, in which businesses and government services depend and could provide better cyber protection.

In this regard, the development and implementation of the Mauritian cybersecurity strategy and the main challenges that were encountered, will be reviewed. The Mauritian cybersecurity strategy was developed following a national survey conducted in October 2013 to assess the security posture of businesses in Mauritius. The aim of the strategy is to make the Mauritian cyberspace more secure and resilient, focusing on the following strategic guidelines:

WELCOME

FOR A RESILIENT AND SECURE MAURITIUS

security

National Cyber Security Strategy
Validation Workshop

24th March 2014
Conference Hall A, Cyber Tower 1, Ebene

National Computer Board

CERT-MU

Stakeholder(s) discussion during the National Cybersecurity Strategy Validation Workshop, Ebene, Mauritius

1. Securing the cyberspace and establishing a front line of defense against cybercrime;
2. Enhancing resilience to cyber-attacks and be able to defend against the full spectrum of threats;
3. Developing an efficient collaborative model between the authorities and the business community to advance national cybersecurity and cyber defense; and
4. Improving the cyber expertise and the comprehensive cyber security awareness of the society at all levels.

Based on the above guidelines, the strategy describes an action plan that provides reasonable assurance of resilience and security to support national missions and economic stability. Twenty-eight (28) projects were identified and some of the key priorities include: (1) the protection of critical information infrastructures, (2) a clear governance framework, (3) the creation of public and private partnerships, (4) fight against cybercrime by developing law enforcement capability, (5) the improvement of the legal framework, and (6) international and regional cooperation on cybercrime. The emphasis was also laid down on the monitoring of the cyber territory for malicious traffic by setting up a cyber-threat monitoring system.

Development and Implementation of the Strategy

Strategy development and implementation is a daunting task and requires the coordination and support of all stakeholders. A few of the issues and challenges faced in bringing the strategy to life, which was developed and approved in 2014 are as follows:

- **Legal basis for project(s)implementation**

A legal basis is an important aspect for the implementation of the projects of the national cybersecurity strategy, and it should be kept in mind while undertaking the legal framework assessment exercise. The take up of amendment of legal provision(s) in the existing legislation or creating new ones at the time of project implementation could be a taxing affair and may derail the set targets. This could even lead to a failure of the project.

- **Inter-institutional collaboration and assignment of stakeholdership roles**

Ownership and the stakeholdership are the vital threads of the strategy development and require a concrete analysis to come up with an actionable plan involving public and private sector that could be realized.

“Many countries recognise the importance of cybersecurity and it has become a national priority”

The exercise requires lengthy discussions and validation procedures before establishing roles and responsibilities of the institutions according to their mandate.

- **Setting up the Public-Private Partnership (PPP) Framework**

One of the core elements of a national cybersecurity strategy is the public-private partnership (PPP). The PPP framework consists of various stakeholders from the public and private sector. It involves a collaborative effort of all key players to safeguard the cyberspace from attacks. It establishes a common scope and objectives and uses defined roles and work methodology to achieve shared goals. However, the implementation of the PPP framework is challenging, as it requires a proper balance between roles and responsibilities to be defined for proper execution and setup.

- **Budget Estimation for projects**

Accurate budget estimation is key to the successful implementation of the strategy action plan, and requires the consideration of a number of factors, such as technology readiness, infrastructure, and skills availability. The steps associated with the budgeting process are highly dependent on both the estimated length of tasks and the resources assigned to the project. A number of constraints, including financial, political, and organisational, may dictate the methods by which resources, such as personnel, equipment, services and materials, are acquired. This should be carefully taken into account while calculating the budget.

- **Accurate Assessment of Human Resource Requirements**

For the proper implementation of the strategy, it is important to have the right people with the skills needed to execute the projects on time. In this process, it is important that the skill requirement exercise is undertaken through a proper survey and its findings are used to address the HR requirements.

On the closing note, it’s worth mentioning that the cybersecurity strategy development and its proper implementation not only provides a better cyber defense to the cyber territory of a country, but it can also lead to economic and social development. Countries embarking on the strategy development or in the stage of implementation could certainly look into these areas for effective development and implementation of their national cybersecurity strategies.

Conclusion

National cybersecurity strategy making is at a turning point. Many countries recognise the importance of cybersecurity and it has become a national priority. African nations too require national cybersecurity strategies that aim to drive economic and social prosperity and protect the countries’ cyber space against emerging threats. The establishment of a national cybersecurity strategy will help them in creating a better cyber protection. However, there are many challenges associated with the strategy development and implementation and to address these concerns, the Mauritian experience could be helpful to be looked into.

More information:

National Cybersecurity Strategy, Mauritius (2014)

Reviewing Senegal's Cybersecurity Capacity Maturity: a strategic approach

As part of the GFCE initiative "Progressing Cybersecurity in Senegal and West Africa", the Global Cyber Security Capacity Centre (GCSCC), in collaboration with the government of the Netherlands carried out a cybersecurity capacity maturity review in Senegal, premised on its National Cybersecurity Capacity Maturity Model (CMM). After consultations with various stakeholder groups, a report with the findings and recommendations was submitted to the government of the Netherlands and the Ministry of Posts and Telecommunications in Senegal. Key findings show that Senegal is more advanced in developing cybersecurity legal frameworks, training and education, and national infrastructure resilience. Potential areas for enhancement include a national cybersecurity strategy, incident response, crisis management, responsible reporting, and cybersecurity marketplace.

Written by: Global Cyber Security Capacity Centre (GCSCC)

In January 2016, a team from the Global Cyber Security Capacity Centre (GCSCC), University of Oxford, in collaboration with the Dutch Government of the Netherlands, carried out a review of the cybersecurity capacity maturity of Senegal premised on its National Cybersecurity Capacity Maturity Model (CMM). The aim of this effort was to enable the country's government to benchmark and prioritise investments in cybersecurity capacity. The review, hosted by the Ministry of Posts and Telecommunications, was part of the GFCE initiative launched by the Foreign Ministry of the Netherlands and Senegal to exchange expertise that would contribute to addressing cybersecurity issues in Senegal.

During a three-day consultation, the researchers held roundtable discussions with representatives from ten stakeholder groups, including representatives from public sector entities, legislators and policy owners, criminal justice and law enforcement, armed forces, academia, civil society, telecommunications companies, finance sector and the Cyber Task Force. Discussions were premised on the five dimensions of the CMM: policy and strategy; culture and society; education, training and skills; legal and regulatory frameworks; standards, organisations, and technologies.

Following the review, the country review report was submitted to the Ministry of Posts and Telecommunications, presenting the findings across the dimensions critical to build a country's cybersecurity capacity and identifying recommendations for the government.

Key findings

Overall, the maturity of Senegal's cybersecurity capacity across the five dimensions of the CMM varied between the start-up and established stages of maturity. In some areas, such as the dimension on policy and strategy and culture and society, Senegal is just beginning discussions on enhancing the capacity of these factors. For example, while there is no national cybersecurity strategy, national incident response capacity or coordinated awareness campaign, all stakeholders agreed that raising the maturity in these factors would fill much needed gaps in the national cybersecurity landscape.

In other dimensions, such as national education, training and skills and the legal and regulatory frameworks, there was some existing capacity in cybersecurity, but still moving from the formative to the established stage. For instance, several universities in Senegal offer courses in information security and cryptography, but do not yet offer courses in cybersecurity specifically. Similarly, there are aspects of the legal environment that have been adopted in order to mitigate cybercrime. Senegal has already adopted, since 2008, legislation on cybercrime, data protection, and e-transactions, though it was widely agreed that the implementation of these laws varies, thus inhibiting the country from elevating its maturity in this factor.

Finally, we came to understand that the implementation of cybersecurity standards within private companies and public entities and at the national level are frequently dictated by whether the institution is under the purview of an external parent company. If an international company mandates security requirements, then ISO standards are usually adopted, but there are few companies that do so voluntarily.

These findings, while unique to Senegal, are comparable to the experiences gathered in other countries with similar level of development across the world. While cybersecurity is an increasingly recognised priority, specific measures to elevate maturity across the different dimensions are still at the initial levels of development and implementation is not always sufficient yet.

Recommendations

In Dimension 1, which looks at cybersecurity policy and strategy, the development of a National Cybersecurity Strategy, the design and dissemination of a coordinated cyber programme and the development of a national CSIRT were recommended as the key actions for enhancing capacity. In addition, the establishment of a mechanism for regular vulnerability disclosure and information sharing between the public and private sector was emphasised.

> **"The maturity of Senegal's cybersecurity capacity varied between the start-up and established stages of maturity."**

Key recommendations relating to the second dimension, which focuses on cyber culture and society, include the enhancement of efforts at all levels of government to promote understanding of risks and threats, the development of a national awareness raising programme, and the expansion of secure e-government services.

Moreover, cybersecurity education, training and skills are crucial to the development of cybersecurity capacity. Recommendations for this third dimension of the CMM encompass engraining cybersecurity training and education throughout all levels of education, developing a nationally coordinated programme on cybersecurity education and skills development, and providing training for experts on various aspects of cybersecurity, as well as conducting mandatory cybersecurity trainings for board members.

In Dimension 4, which looks at legal and regulatory frameworks and the capacity of the criminal justice system, the GCSCC recommended to review and amend existing laws on cybersecurity, data protection and cybercrime, strengthen national investigation capacity for computer-related crimes, and establish and strengthen international cooperation mechanisms to combat cybercrime.

Finally, recommendations for the enhancement of technology and standards aspects of cybersecurity include the promotion of the adoption of international IT standards, the establishment of a national programme for infrastructure development and the fomentation of sharing information and best practices among organisations.

The full report was submitted to the Ministry and is publically available on the official website of the Ministry of Posts and Telecommunications:

- English version
- French version
- Abstract in French

Next steps

Senegal has since started to define the priorities to enhance the country's cybersecurity capacity and has begun to implement some of the recommendations. This includes the development of the National Cybersecurity Strategy which is supported by the GFCE initiative, until the end of the year (on December 2016). In September 2016, the national digital strategy named SN2025 has been officially validated technically with all Senegalese ICT stakeholders. The document considers the recommendations of the report prepared by the GCSCC. Senegal has also begun to review the framework legacy with a group of national and international experts and to discuss the creation of a National Cybersecurity Center.

A study for the awareness campaign in 2017 is under way. Some stakeholders have been appointed by Senegal and are ready to participate in the campaign.

In 2017, the second regional Experts Meeting is planned as part of the GFCE initiative. It builds upon the first meeting held in Dakar in April 2016 which provided the building blocks for the "Dakar Declaration on Cybersecurity" and whose components cover cybersecurity strategy, incident response teams, legal frameworks, cybersecurity awareness and cybersecurity education. It sets cybersecurity capacity building on the agenda in Africa and is embraced by several African countries and regional organisations.

About

The Global Cyber Security Capacity Centre (GCSCC), University of Oxford, is a leading international centre for research on efficient and effective cybersecurity capacity building, promoting an increase in the scale, pace, quality and impact of cybersecurity capacity building initiatives across the world. With its Expert Advisory Panel and senior academics from various disciplines the GCSCC has created a first-of-its-kind model to review cybersecurity capacity maturity across five dimensions critical to build a country's cybersecurity capacity: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training and skills; legal and regulatory frameworks; and standards, organisations, and technologies.

The National Cybersecurity Capacity Maturity Model (CMM) aims to enable nations to benchmark, better plan investments and national cybersecurity strategies, and set priorities for capacity development. Since 2015, it has been deployed together with the GCSCC's strategic partners (including the Organization of American States, World Bank, the Commonwealth Telecommunications Organisation and the International Telecommunication Union) in more than 40 countries around the world. It also underpinned a regional study in Latin America and the Caribbean through collaboration with the Organization of American States.

Governmental auditing as a catalyst to improve cybersecurity mindset of Latin American and Caribbean governments

Latin America and the Caribbean still have opportunities to improve the cybersecurity mindset of their governments. Recent research shows that a large number of countries in the region have a minimal or basic recognition of this matter. This paper recommends the evaluation of Information Security Risk Management as part of government auditing to help increase the cybersecurity mindset of government.

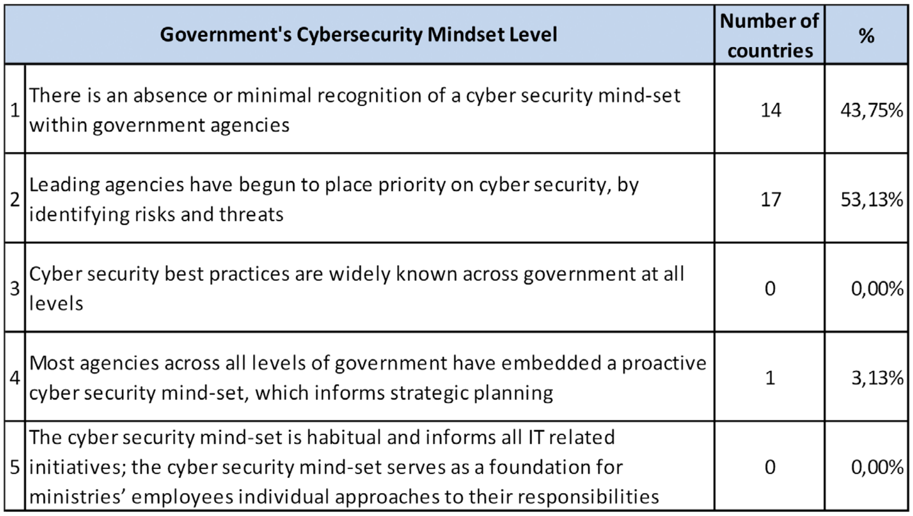
Written by: Jairo Hernan Marin Agudelo, Juan Carlos Buritica Grajales, Carlos Andrés Arbelaez Velasquez. Auditors at Comptroller General's Office of Medellin, Colombia

Cybersecurity mindset of Latin American and Caribbean governments and the trust in e-government

In 2016 the collaboration between the Inter-American Development Bank (IDB), the Organization of American States (OAS), and the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, produced a cybersecurity report entitled **"Cybersecurity Are we ready in Latin America and the Caribbean?"** [1]. This report presents an up-to-date holistic picture of the state of cybersecurity of countries in Latin America and the Caribbean. It was carried out using an online tool to gather data from cybersecurity stakeholders representing different sectors.

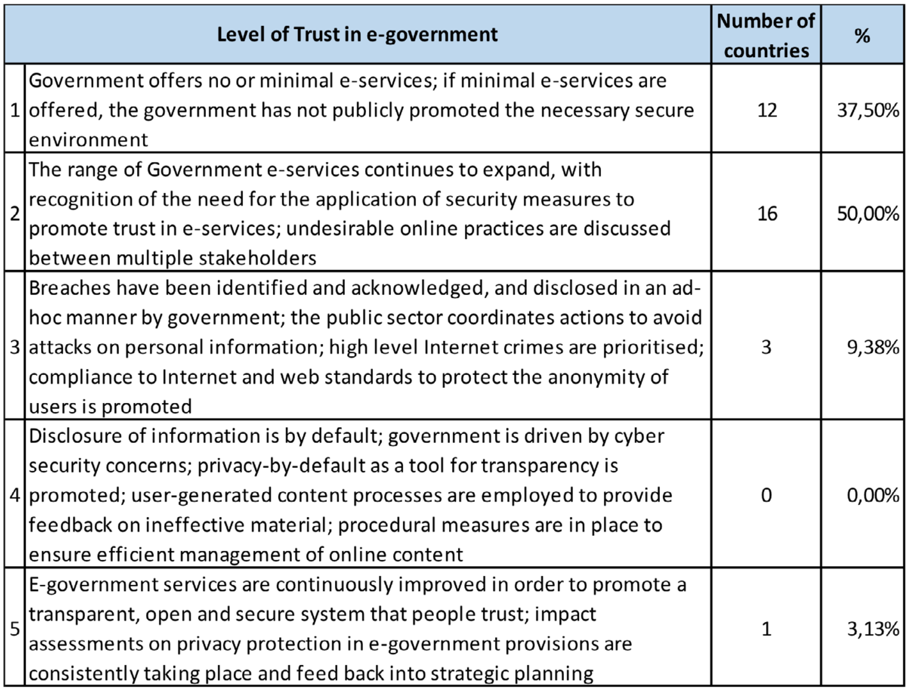
As part of the report, the collected data was analyzed using the 49 indicators of the Cybersecurity Capability Maturity Model (**CMM**) developed by the **GCSCC** [2]. In this model, the indicators are divided into five dimensions, with "Cyber Culture and Society" being one of them. Each dimension is divided into factors, and each factor into indicators. Finally, in order to determine the level of maturity, each category has a set of indicators across five levels: 1. Start-up; 2. Formative; 3. Established; 4. Strategic; and 5. Dynamic (see Table 1 and Table 2).

Regarding the results obtained and presented in the report, some of the most interesting aspects are: government cybersecurity mindset and the Trust in e-government. The first



	Government's Cybersecurity Mindset Level	Number of countries	%
1	There is an absence or minimal recognition of a cyber security mind-set within government agencies	14	43,75%
2	Leading agencies have begun to place priority on cyber security, by identifying risks and threats	17	53,13%
3	Cyber security best practices are widely known across government at all levels	0	0,00%
4	Most agencies across all levels of government have embedded a proactive cyber security mind-set, which informs strategic planning	1	3,13%
5	The cyber security mind-set is habitual and informs all IT related initiatives; the cyber security mind-set serves as a foundation for ministries’ employees individual approaches to their responsibilities	0	0,00%

Table 1: Government´s Cybersecurity Mind-set Level.
Source: authors, using data from Observatory of Cybersecurity in Latin America and the Caribbean



	Level of Trust in e-government	Number of countries	%
1	Government offers no or minimal e-services; if minimal e-services are offered, the government has not publicly promoted the necessary secure environment	12	37,50%
2	The range of Government e-services continues to expand, with recognition of the need for the application of security measures to promote trust in e-services; undesirable online practices are discussed between multiple stakeholders	16	50,00%
3	Breaches have been identified and acknowledged, and disclosed in an ad-hoc manner by government; the public sector coordinates actions to avoid attacks on personal information; high level Internet crimes are prioritised; compliance to Internet and web standards to protect the anonymity of users is promoted	3	9,38%
4	Disclosure of information is by default; government is driven by cyber security concerns; privacy-by-default as a tool for transparency is promoted; user-generated content processes are employed to provide feedback on ineffective material; procedural measures are in place to ensure efficient management of online content	0	0,00%
5	E-government services are continuously improved in order to promote a transparent, open and secure system that people trust; impact assessments on privacy protection in e-government provisions are consistently taking place and feed back into strategic planning	1	3,13%

Table 2: Level of Trust in e-government.
Source: authors, using data from Observatory of Cybersecurity in Latin America and the Caribbean

one is analyzed on the “Cybersecurity Mind-set” factor by the “Government” category and the second one is analyzed on “Confidence and Trust on the Internet” factor by the “Trust in e-government” Category.

Pertaining to the government cybersecurity Mind-set, the report shows that 96.88% of the 32 countries analyzed in Latin America and the Caribbean, have an assessed level of maturity rated at 1 or 2 (see Table 1). In addition to the trust in e-government, the report shows that 87.5% of the 32 countries analyzed, have an assessed level of maturity of 1 or 2 (see Table 2). (Source: authors, using data from Observatory of Cybersecurity in Latin America and the Caribbean.

These results indicate that there are still opportunities to improve the cybersecurity mindset within the Latin American and the Caribbean governments, and also to improve the confidence with citizens in the services they offer.

Government auditing as one way to help increase the cybersecurity mindset of government

The Government auditing has been one of the most important mechanisms used across the world to monitor the way in which taxpayers' money is spent. Traditionally, it has been focused on the economy, effectiveness and efficiency of government actuations and operations.

Nowadays, as a consequence of the digital revolution, there has been a change in the way in which the government and the citizens interact. The Information and Communication Technologies (ICTs) have been used to improve services deployment and covering, and even have been used to offer online transactions to citizens. According to Organization of American States -OAS-, this application of ICTs to government functions and procedures with the purpose of increasing efficiency, transparency and citizen participation, is called e-government. Obviously, this new approach impacts the traditional way in which government has operated, and therefore also has an impact on government auditing.

It is neither effective nor efficient if government spends taxpayers' money to implement online services that are not available when citizens need them, nor when the services are scarcely used because the citizens do not trust them. One way to evaluate effectiveness and efficiency of government actuations in e-government environment is to control that government online services will be accessible to users during planned hours of operations, and they are also reliable enough to make citizens want to use them.

One of the most widely accepted practices used to obtain an acceptable level of service reliability and availability regarding online services, is to perform an adequate Information Security Risk Management **(ISRM)**. As a result, it is reasonable that government auditors look for evidences from an appropriate **ISRM** on government online services, and not only in the financial information systems.

The regular application of government auditing has promoted beneficial changes for the audited matter. Because of the rigorous control applied by the auditors on government financial operations over the years, the government functionaries are very diligent about executing these operations with great care. The regular application of government auditing on **ISRM** could also promote beneficial changes, like a more careful design, implementation and operation of online services.

The findings derived from auditing normally generates improvement actions, which the government agencies and functionaries are responsible for implementing. In this way, giving more importance to **ISRM** with respect to government auditing could help to improve the security of online services, and also the cybersecurity mindset of government functionaries and agencies. In addition, it is reasonable to think that more secure government online services, will increase citizens' confidence in e-government and their use of government online services.

More information:

[1] Observatory Cybersecurity in Latin American and the Caribbean. (2016). Cybersecurity Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report. [PDF].

[2] Global Cyber Security Capacity Centre, University of Oxford. (2014). Cyber Security Capability Maturity Model (CMM) – V1.2, (2014) [PDF].

“Pokémon Go” and Legal Implications in Brazil

The launching of new games always causes excitement, but the level of access to personal and sensitive data may bring risks. Do players know this?

Written by: Renato Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados

Gone is the time when social isolation was the main villain for the online game critics. Nowadays, online games incorporated physical elements, with players interacting with other people in different environments, with very real dangers.

This is exactly the case of the polemic and commented game Pokémon GO. Counting on numberless players of several countries, the game has been causing enthusiasm by allowing players, through data geolocation and users’ smartphone cameras, to hunt little monster on city streets in heightened reality environments.

The idea of going around to catch game creatures (the so-called ‘pokémon’) in public environments may even be interesting to get people out of their houses. However, the frequency of accounts of absurd situations arising from playing the game is startling. Since the reporting of cases of trickery, falling into precipice, robberies and so on, addiction to this game has effectively generated consequences that go way beyond virtual manipulation of bits and bytes. In fact, the legal implications have already begun to be noticed:

1. Level of Access to User Information

As it usually happens with all services of this nature, in order to access Pokémon GO the interested party must provide data and authorize the game’s holding company. In this game’s case, the degree of access to information is enormous, based on the description of the policies appearing on the company’s official website (www.pokemongo.com). According to the company’s Terms of Use, in addition to personal data, information based on localization and photographs are shared with the company, and players agree to the use of cookies, web beacons, and push notifications, among others. Everything is stored in the United States and, depending on the case, it can be shared with unintended parties on the part of the user. Other kinds of information, such as age, date of birth, gender, nationality, hobbies, and preferences may be collected and associated with the player’s personal data.

As it can be seen, in possession of all this information, Pokémon GO will know more about some young people than their own parents will. It remains to be found out if it is with absolute awareness that people are providing all these authorizations, since the reading of the terms and conditions is not a very familiar habit to the majority of web users. Therefore, the question is: would it not be too risky, only for entertainment purposes, to combine and share with a single service supplier so much personal information?

2. Data Technical Safety

On its website, the gaming company informs of the caution and technical certifications applicable to the safety of client data, which seem satisfactory. Nevertheless, considering that it is impossible to ensure with 100% certainty that hackers will never have access to the system, what can happen if all this identifiable data "leaks"? The problem here is that the level and detail of personal data are high (e.g., physical routes, preferred places, hobbies) and, if used for illegal purposes, they can compromise even the players' physical safety.

3. Adventures through the City

Although people have a relative knowledge about the differences between public and private places, to players it is always good to remember: environments with access to the public are not necessarily synonyms of public spaces. That is: many open places of access to the public (e.g., churches, malls, commercial establishments) are private and follow access rules determined by the proprietors, which may restrict players' access and use. Additionally, religious temples, for instance, usually enjoy special legal protection and cannot have any inconvenience caused by eventual people in search of their virtual monsters. Some places have also restriction rules for cameras or cell phones for the preservation of author and image rights (e.g., cinemas, theaters) and, therefore, the practice of this game in these environments may bring problems to the most insistent gamers.

4. Possibility of Damage Liability

In Brazil, the Civil Rights Framework for the Internet and the Consumer Defense Code decisively establish [1] the service provider's obligation to provide technical safety and data privacy for its clients. Equally, in the other countries where Pokémon Go was launched certainly there are similar protection rules. Therefore, more than a voluntary measure, it is up to the holding company of Pokémon GO the duty to safeguard the inviolability of the ocean of data collected from its users. Damages arising from these services may evidently be the objects of legal liability, implicating the taking of applicable legal measures.

Finally, it cannot be denied that while the gaming world in general, serves as entertainment , it must be lived/carried out with responsibility and under the legal limits. Furthermore, besides the necessary reflection on the reasonable risks that each one is prepared to assume on the leisure activities, it is important to emphasise that the new games may put people on the streets and in motion, but good sense can never be forgotten at home.

More information:

[1] Law 12.965/2014 – Brazilian Civil Rights Framework for the Internet: items II and III of article 3 and article 10; Law 8.078/1990 - Brazilian Consumer Defense Code: article 4.

Australia's $230M Cyber Security Strategy

Advancing and protecting Australia's interests online

Australia's Cyber Security Strategy was announced by the Prime Minister, the Hon Malcolm Turnbull MP on 21 April 2016. The Strategy sets out five themes for Australia's cyber security from now to 2020 and is supported by a $230 million investment in practical initiatives. The Strategy will be implemented with the assistance of a newly appointed Minister Assisting the Prime Minister on Cyber Security and Special Adviser to the Prime Minister on Cyber Security.

Written by: Office of the Cyber Security Special Adviser, Australia

Australia's 2016 Cyber Security Strategy builds on Australia's 2009 Strategy to embrace opportunities created by cyberspace and reinforce Australia's role as an international leader in cyber security. In launching the Strategy on 21 April, Prime Minister the Hon. Malcolm Turnbull MP, spoke of the Internet's transformational impact on Australia and the world: "there is no global institution or infrastructure more important to the future prosperity and freedom of our global community than the Internet itself."

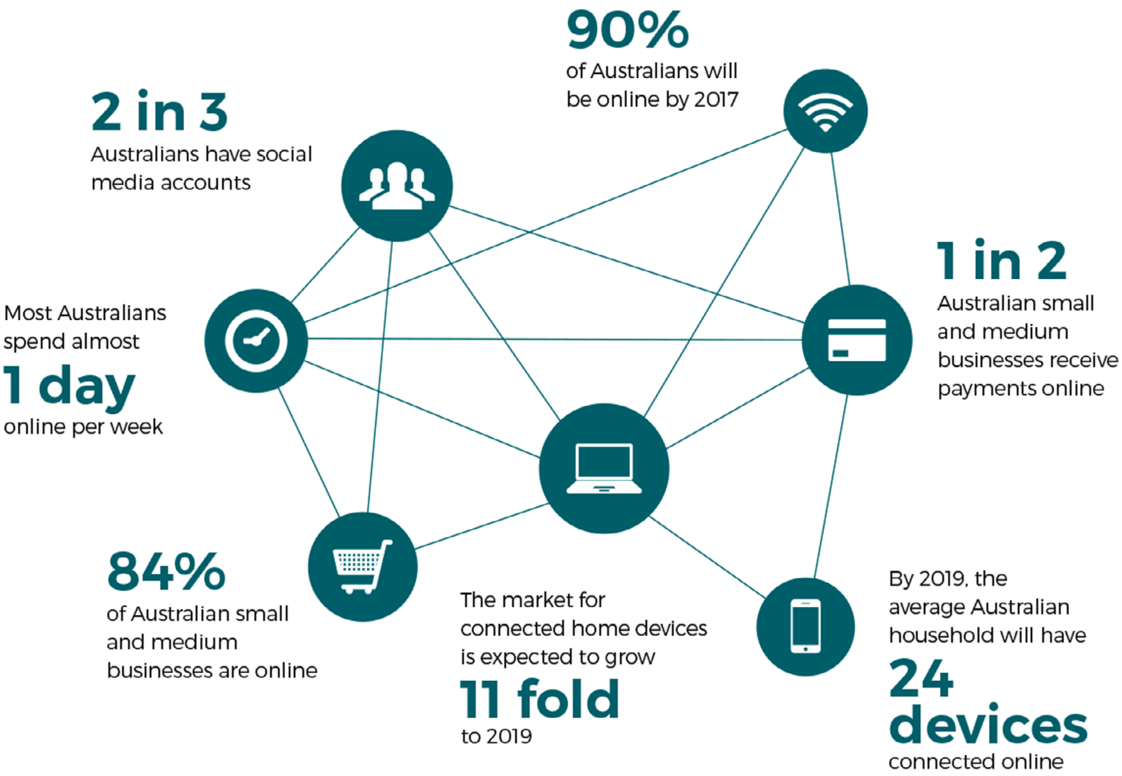
Online and mobile technology are both essential for business growth and connecting people across all sectors of society, in their private, commercial and government interactions. Australia has been quick to benefit from the growth and expansion of the Internet: in 2014, the Internet-based economy contributed $79 billion to our national economy, a figure which is rapidly growing.

The Strategy charts a clear role for the Australian Government to grow Australia's cyber security capability, to anticipate and to respond to cyber threats and to work internationally to promote norms of behaviour that are consistent with a free, open and secure Internet. Working with the private sector, which owns the infrastructure, the Australian Government is also leading the effort to ensure all Australians have an understanding of the real-world impacts of cyber risks and the way they affect our current and future prosperity. Australians will have the cyber security skills and knowledge to thrive in the digital age.

Five Action Themes

The Australian Government's Cyber Security Strategy sets out five themes to strengthen Australia's cyber security from now to 2020:

1. **A national cyber partnership:** set and drive the strategic cyber security agenda through engagement with business and the research community and streamlining cyber security governance.
2. **Strong cyber defences:** raise the bar on cyber security performance and encourage sharing threat


90%
of Australians will be online by 2017
2 in 3
Australians have social media accounts
1 in 2
Australian small and medium businesses receive payments online
Most Australians spend almost
1 day
online per week
84%
of Australian small and medium businesses are online
The market for connected home devices is expected to grow
11 fold
to 2019
By 2019, the average Australian household will have
24 devices
connected online

Australians are becoming increasingly connected online Credits: Department of the Prime Minister and Cabinet

information within public and private sectors.

3. **Global responsibility and influence:** champion an open, free and secure internet with our international partners and build capacity in our region and globally.
4. **Growth and innovation:** support the cyber security sector to diversify and develop new markets and allow all businesses to grow and proposer through cyber innovation.
5. **A cyber smart nation:** improve cyber security awareness, address skills shortages and develop a highly-skilled cyber security workforce.

Each theme is supported by actions for the Government and private sector. Many of these actions recognise that no single sector – Government, business, academia or the general community – can of itself ensure cyber security. Cyber security is a global challenge that requires innovative thinking, creative solutions and engagement with all sectors of Australian society.

"Only by acknowledging, explaining and analysing the problem can we hope to impose costs on perpetrators and empower our private citizens, government agencies and businesses to take effective security measures", Prime Minister the Hon Malcolm Turnbull MP, launch of Australia's Cyber Security Strategy, 21st April 2016.

Practical initiatives

The Strategy is supported by a $230 million investment in practical initiatives co-designed with the private sector. These include: establishing Joint Cyber Security Centres to share threat information between government, the private sector and academia; appointing a Cyber Ambassador to lead international engagement on cyber issues; and launching a Cyber Security Growth Centre with the private sector to co-ordinate a national cyber security innovation network.

The capability of Australian Government agencies to protect the Australian community by investigating and responding to cyber incidents is being enhanced through extra resources for Australia's natio-

Australian Government
AUSTRALIA'S
CYBER SECURITY STRATEGY
cybersecuritystrategy.dpmc.gov.au
#CyberStratAus
Enabling innovation, growth & prosperity

Prime Minister Turnbull launches Australia's Cyber Security Strategy

> **"There is no global institution or infrastructure more important to the future prosperity and freedom of our global community than the Internet itself."**
>
> Hon. Malcolm Turnbull MP

nal Computer Emergency Response Team (CERT Australia) and law enforcement agencies. The Strategy will also fund several collaborative initiatives such as joint exercises with the private sector, voluntary guidelines promoting good cyber security practice and voluntary cyber security governance health checks for ASX-100 listed companies.

Implementing Australia's strategy is a national priority being driven by the executive and the national cyber security key actors within Government. Australia recognises and embraces the massive opportunities presented by the digital age. Australia's new Cyber Security Strategy underpins that potential by cementing Australia's role in protecting the online communications environment.

A key challenge for the strategy's implementation is finding solutions to keep pace with the rapid growth of the technology industry. The Strategy must remain strategic by being responsive—a mere plan is insufficient for guiding Australia through the digital age. Strong and robust relationships with the private sector and academia are essential to co-designing successful initiatives and ultimately addressing the challenge of keeping pace. Engagement with these sectors, in new ways, has already begun and will unlock the potential of a free, open and secure internet.

A New Digital Era and the Need to Protect Critical Societal Functions

The EU Cybersecurity Strategy adopted in 2013 identified important gaps across the European Union in terms of national capabilities, coordination in cross-border incidents, and private sector involvement and engagement. On 6 July 2016 the NIS Directive [1] was adopted in response to this identified need. On the eve of the adoption, the European Commission signed a contractual Public-Private Partnership (cPPP) with the EU's cyber security industry, in order to better equip Europe against cyber-attacks and to strengthen the competitiveness of its cybersecurity sector.

Written by: Mr. Christer E. Hammarlund, Cyber Defence Policy Officer at the Cybersecurity and Digital Privacy Unit of the European Commission's Directorate General for Communications Networks, Content and Technology (DG CONNECT).

With the digital economy making headway across the globe, mobile communications and the Internet are now pervasive in every business and service sector all over the world, as well as in our private lives. Companies fighting for a competitive edge are increasingly presenting their customers with digital solutions. The number of Internet users worldwide has tripled over the past decade, and broadband and smartphones are faster, cheaper, and more widespread. However, with the digital economy comes the inevitable issue of security.

The NIS Directive

In 2013, the European Union adopted the Cyber Security Strategy and launched a legislative proposal (known as the 'NIS Directive') with the objective to bring cybersecurity capabilities at the same level of development across all the EU Member States and ensure efficiency in the exchanges of information and cooperation both nationally but also at cross-border level. The Directive was finally adopted by the European Parliament on 6 July this year, and is now awaiting Member State implementation. The NIS Directive is the first EU-wide cyber security directive of its kind.

The need for such a legislative framework has become more pressing in light of ongoing developments in this field. For example, according to a recent survey, the number of security incidents across all industries worldwide rose by 38% in 2015 while at least 80% of European companies experienced at least one cybersecurity incident over the past year.

The Directive's first objective is to

Günther H. Oettinger, European Commissioner for the Digital Economy and Society, signing the new Public-Private Partnership with industry, 5 July 2016. Credits: European Commission.

increase national cyber security capabilities. This will be achieved through Member States developing a national strategy on NIS, the formation of an NIS national authority, and the launch of a Computer Security Incident Response Team (CSIRT).

Secondly, the Directive aims to improve EU-level cooperation by setting up a Cooperation Group for strategic cooperation among the EU Member States, the European Commission (acting as the secretariat), and the EU Network and Information Security Agency (ENISA). There will also be a CSIRT network for operational cooperation between the national CSIRTs, CERT-EU, and ENISA (acting as the Secretariat).

Thirdly, the Directive aims to cover the main risks by working to protect the most critical networks in society, known as Operators of Essential Services (EOSs). These include sectors such as energy, water, health, transport, banking, financial markets (e.g. trading venues, central counterparties), digital infrastructure (e.g. internet exchange points, domain name system service providers, top level domain name registries), and certain digital businesses that are considered to be of general importance when it comes to cyber security (so called 'digital service providers', “The European Commission is also working to strengthen industrial capabilities in Europe”

or DSPs); online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online), cloud computing services and search engines. These operators will be required to report serious incidents to their pertinent national authorities.

The first European PPP on cybersecurity

In parallel, other initiatives are brought forward to better equip Europe address cyber threats and improve the competitiveness if its cybersecurity sector. A flagship initiative in this field and first of its kind in Europe is the now up-and-running contractual Public-Private Partnership (cPPP) on cyber security. Under the EU’s research and innovation programme (“Horizon 2020”), the EU has pledged to invest 450 million Euro in this partnership between the European Commission and the European Cyber Security Organisation that represents European cybersecurity market players. The cPPP includes 150 stakeholders from business, academia and research in Europe, forming an ecosystem in cyber security. The PPP will help European industry tackle cyber threats, strengthen cooperation across the EU, and trigger up to Đ1.8bn of investment by 2020.[2]

Need for additional, complimentary measures

The European Commission is also working to strengthen industrial capabilities in Europe by addressing the current cybersecurity market fragmentation. To this end, a possible European certification framework for ICT security products is another measure currently under consideration, while there is recognition for the need to support innovative cybersecurity SMEs scale up their operations by facilitating their financing, potentially through the EU investment plan. Evidently, the rapidly evolving cybersecurity landscape calls for a comprehensive set of measures that address the multi-sectoral nature of the cybersecurity challenges at hand.

More information:

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1, 19.7.2016.

[2] http://europa.eu/rapid/press-release_IP-16-2321_en.htm

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ('NIS Directive')

EU’s Digital Single market Strategy

European Commission Communication “Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry”, of 5 July 2016

European Union Agency for Network and Information Security (ENISA)

OCTOBER CYBERSECURITY AWARENESS MONTH

October 2016 marked the 13th annual National Cyber Security Awareness Month. Together with interested partners, the GFCE members pursue opportunities for collaboration on raising cybersecurity awareness around the globe. Under the GFCE Initiative to build a Global Campaign to Raise Cybersecurity Awareness, global adoption of October as National Cyber Security Awareness Month is encouraged by Canada, the OAS and the United States as a way to increase citizens' understanding of cyber threats by empowering them to adopt safer and more secure practices online.

NORTH AMERICA, LATIN AMERICA AND THE CARIBBEAN

Did you know? Colombia, Dominica, Jamaica, Panama, Paraguay and Uruguay signed the STOP.THINK.CONNECT messaging convention and four other countries already began the process of becoming partners.

Four countries in LAC adopted national cybersecurity strategies with a focus on awareness raising and seven others are in the process of developing a national cybersecurity framework.

In partnership with the U.S. Government and various partner organizations, the National Cyber Security Alliance, a U.S. non-profit, released a new awareness campaign focused on helping people protect their online accounts and increase their cybersecurity awareness. The Lock Down Your Login Campaign describes how users can protect their online accounts using strong authentication techniques, including the use of biometrics or a security key. For more information on cybersecurity awareness efforts, visit (https://www.lockdownyourlogin.com) and (https://www.dhs.gov/stopthinkconnect)

During the first week of October, Public Safety Canada launched Cyber Security Awareness Month and cyber security with the Get Cyber Safe campaign (https://www.getcybersafe.gc.ca/index-en.aspx).

General links

https://www.gosafeonline.sg/
https://cybersecuritymonth.eu/
https://staysafeonline.org/ncsam/about (U.S.)
https://www.dhs.gov/stopthinkconnect (U.S.)
http://www.nisc.go.jp/security-site/campaign
https://www.dhs.gov/national-cyber-security-awareness-month (U.S.)
https://stopthinkconnect.org/get-involved (Partner brochure STOP.THINK.CONNECT)
http://www.getcybersafe.gc.ca/cnt/rsrcs/csam-tlkt-en.aspx (Canada - infographics/banner)
https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersafety_Awareness_Southafrica_0.pdf

EUROPE

European Cyber Security Month (ECSM) marked its 5th anniversary with a kick-off event in Brussels on September 30th, 2016. A total of 455 activities across 31 European countries took place during October. https://cybersecuritymonth.eu/

Did you know? In recognition of Cyber Security Month, ENISA hosted 100 of the best young security talents from 10 different nations for the title in the finale of the European Cyber Security Challenge in Düsseldorf, Germany. The team from Spain secured the first place. ECSC 2017 will be held in Spain next year. (http://www.europeancybersecuritychallenge.eu/2017/join/)

The largest and most comprehensive EU cyber-security exercise to date, Cyber Europe 2016, occurred on 13-14 October with the participation of more than 700 cybersecurity professionals from 30 EU and EFTA countries and over 300 organizations.

ASIA-PACIFIC

Japan celebrated, in collaboration with other governments of the ASEAN countries, an international cybersecurity campaign focused on increasing citizens' interest and deepening their understanding in cybersecurity. (http://www.nisc.go.jp/press/pdf/campaign2016.pdf).

Did you know? Singapore International Cyber Week was built around the annual GovernmentWare (GovWare) cyber conference? The theme was "Building a secure and resilient digital future through partnership" and was held October 10-12. (https://www.sicw.sg/#home).

AFRICA

Nigeria: Under the aegis of the Centre for Cyber Awareness and Development (CECAD), a NGO has called on the federal government to adopt October as the Nigerian National Cybersecurity Awareness Month.

Ghana: In November, Ghana held a week of cybersecurity events that covered public-private partnerships, basic awareness raising, and concepts of incident management.

The ICC Cyber security guide for business

Helping companies rise to the challenge

Launched at the Global Conference on Cyberspace in 2015, the International Chamber of Commerce (ICC) Cyber security guide for business offers a simple process for raising awareness for online security. It is designed to be a conversation starter between information technology specialists and company management in order to guide enterprises of all sizes and sectors on ways to address cyber security challenges and to engage the companies in their supply chains to also tackle these issues.

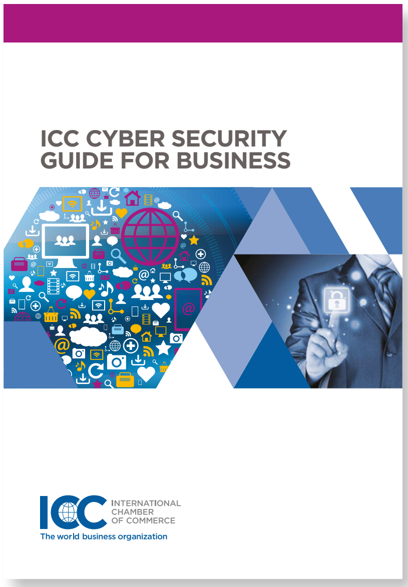
Written by: Gerard Hartsink, representative of the International Chamber of Commerce (ICC) Commission on the Digital Economy to the GFCE and Chair ICC Taskforce Cyber Security

Modern information and communications technologies are enabling business of all sizes to innovate, reach new markets and drive efficiencies that benefit customers and society. Yet, increasingly, business practices and policies are stressed while adapting to the direct and indirect impacts of pervasive communication environments and network information flows that are required in the delivery of goods and services. Many enterprises adopt modern information and communications technologies without fully realizing that new types of risks must be managed.

Failures in cyber security are constantly in the press with reports of malicious actors breaching enterprises, both large and small – seemingly at will and with ease. From a business perspective, it is vital that a company – large or small, click-and-mortar or high-tech – be able to identify their cyber security risk and effectively manage threats to their information systems. At the same time, all business managers spanning from directors of small family business to executives of large multinational companies must recognize that absolute security is an elusive goal. Unlike many business challenges, cyber security risk management remains a problem with no easy fix available.

Cyber security risk management: a collaborative and ongoing process

An array of documents and guidelines trying to help users understand and mitigate these risks already exists. However, the sheer volume of available material poses a challenge itself. For end users and businesses alike it can be difficult to know what to start reading and what kinds of documents are appropriate to their particular needs. The range spans from comprehensive explanations on top cyber threats tailored for technical ex-


ICC CYBER SECURITY
GUIDE FOR BUSINESS
ICC INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

ICC Cyber security guide for business

perts to boardroom one-pagers often mistakenly perceived as a quick-fix, to a seemingly daunting problem that rather requires a consistent application of management attention with a tolerance for bad news and discipline for clear communication.

With many excellent resources already available, suitable material to assist business management in their approach to cyber security still remains scarce. The International Chamber of Commerce (ICC) Cyber security guide for business addresses this gap and outlines how enterprises of all sizes can identify and manage cyber security risks.

This pragmatic guide stands out as the first of its kind to be issued by an international business organization. It is first and foremost a conversation starter developed to help business management of companies of all sizes and sectors frame cyber security discussions with information technology professionals - and vice versa - to put a collaborative and ongoing management approach in place.

The concepts outlined in the guide help companies overcome fears and improve risk awareness to rise to the information security challenge of this fast changing environment as well as to engage the companies in their supply chains to also tackle these issues.

Five principles to identify risks, six key actions companies should take

Produced by the International Chamber of Commerce (ICC) Commission on the Digital Economy, the ICC Cyber security guide for business is informed by global cyber security guidelines and national strategies offering businesses a framework to consider the question of security online. It starts out with five principles that help enterprises identify cyber security risks and drawing on various sources and best practices, goes on to pin point six key actions that companies should be sure to take.

While approaches to information security may differ from company to company depending on a number of factors, there are a number of high-level principles that inform sound information security practice for all companies, independent of size or industry. The five key principles presented in this guide relate firstly to the vision companies should adopt, such as thinking of information security in its broadest sense, not just in terms of information, and approach the resilience of the company to cyber risks holistically by improving company culture and employee mind-set towards cyber security risk management practices. Secondly, the principles outline the organization and processes companies should follow such as being prepared to respond to a breach, demonstrating a leadership commitment and act on their vision for cyber security risk management to ensure its implementation.

The six key actions show how these principles translate to practicalities. They call on companies to back up business information and validate restore process; update information technology systems; invest in training; monitor their information environment; layer defenses to reduce risk; and prepare for when the breach occurs.

The guide also helps companies convert their vision into implementation by discussing how these principles can be applied into policies to facilitate the development of an enterprise's cyber security risk management activities.

The guide features a self-assessment questionnaire as well, a simple checklist as a tool for management to help guide their internal review of their company's cyber resilience capabilities regardless of whether they are just beginning in their information security initiatives or are looking to identify remaining gaps or vulnerabilities and paths to improvement within their respective company.

Used periodically, the guide and questionnaire will enable managers to ask the right questions to the teams involved in these initiatives and proactively partake in the development of the best-fitting approach for their specific business to prepare and manage cyber incidents.

Available resources

Launched at the Global Conference on Cyberspace in 2015, the ICC guide is now available in English, French and Spanish and has a locally

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

ICC Cyber security Guide for Business

6 SECURITY ACTIONS

ACTION 1
Back up business information; validate restore process

ACTION 2
Update information technology system

ACTION 3
Invest in training

ACTION 4
Monitor your information environment

ACTION 5
Layer defences to reduce risk

ACTION 6
Prepare for when the breach occurs

6 security actions for business

adapted Dutch version. It is distributed through ICC's global network of national committees, member companies, business associations and chambers of commerce, spanning over 130 countries and is also available for download free of charge on the ICC website. The website also features an online appendix of resources to complement the guide serving as a living resource to provide more specific advice as these materials are developed - from standards of practice to technical standards and more.

ICC has a proud, nearly hundred-year history of providing companies with tools and self-regulatory guidance to promote good business practice. As the world business organization, whose membership is composed of enterprises from all sectors and regions, ICC developed this simple, clear guide to help business play their part in addressing the increasingly serious challenge of cyber security. ICC is an organization dedicated to facilitating trade and investment, and fostering confidence in the digital economy and increasing the considerable opportunities that it brings to business, consumers, governments and society.

Since its launch in April 2015, the ICC Cyber security guide for business has reached companies – large and small – from India to Brazil, from Finland to South Africa. It has proven its versatility by serving as input material for large conferences at venues such as the World Bank or the Internet Governance Forum as well as training material for local businesses in Spain and Morocco and awareness-raising material for SMEs and chambers of commerce at the World Chambers Congress 2015.

Reception to the guide has been extremely positive as there is a recognized need for businesses to be more security-savvy. This matter has long outgrown just IT departments and is increasingly reaching the boardrooms of companies. However, from this example in the U.K. for instance, where businesses have doubled expenditure on security budgets in recent times yet remain unaware of the number or source of cyber incidents that struck their businesses over the past year [1], the need for more dialogue between the two camps, is highlighted as a business risk. The ICC Cyber security guide for business aims exactly at the heart of the matter by offering a tool for identifying both what to discuss and how to approach this much needed dialogue in a way that is relevant from both perspectives.

Download the ICC Cyber security guide for business.

More information:

[1] PwC: The Global State of Information Security® Survey 2017

The Budapest Convention on Cybercrime: a framework for capacity building

The Convention on Cybercrime of the Council of Europe was opened for signature in Budapest in November 2001. Fifteen years later, it remains the most relevant international agreement on cybercrime and electronic evidence. Membership keeps growing, while both the quality of implementation and the level of cooperation between Parties keep improving, and the treaty itself is evolving to meet new challenges. The formula for success is a "dynamic triangle"; The Budapest Convention is complemented by an effective follow up mechanism and by capacity building programmes, which are fed back into the Committee, contributing towards the Convention's evolution. The leitmotif of this approach is "to protect you and your rights in cyberspace."

Written by: Alexander Seger is Executive Secretary of the Cybercrime Convention Committee and Head of the Cybercrime Division at the Council of Europe in Strasbourg, France.

Building on agreement

Cybercrime has been around for more than 40 years. The Council of Europe had been dealing with this topic from a criminal law perspective from the mid-1980s onwards. By 2001, the issue had become sufficiently important to warrant a binding international treaty. Negotiated by the member States of the Council of Europe together with Canada, Japan, South Africa and the United States of America, the Convention on Cybercrime was opened for signature in Budapest, Hungary, in November 2001.

Since then, information and communication technologies (ICT) have transformed societies worldwide. They have also made them highly vulnerable to security risks such as cybercrime.

While there is recognition of the need to strengthen security, confidence and trust in ICT and to reinforce the rule of law and the protection of human rights in cyberspace, all things "cyber" have now become too important. As they touch upon fundamental rights of individuals as well as national (security) interests of States, it is increasingly difficult to reach international consensus on common solutions.

In order to overcome this dilemma, the most sensible approach is to focus on common standards that are already in place and functioning, such as the Budapest Convention on Cybercrime, and on approaches on which

Cybercrime Convention Committee (T-CY), Plenary session, May 2016. Credits: Council of Europe

there is broad agreement, in particular, capacity building.

Common standards: the Budapest Convention

The Budapest Convention is a criminal justice treaty that provides States with (i) the criminalisation of a list of attacks against and by means of computers; (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and (iii) international police and judicial cooperation on cybercrime and e-evidence.

It is open for accession by any State prepared to implement it and engage in cooperation. By November 2016, which marked also the 15th anniversary of the Convention, 50 States were Parties (European countries as well as Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and the USA). Another 17 from all regions of the world had signed it or been invited to accede.

Assessments and follow up: Cybercrime Convention Committee

These States that currently amount to 67, together with ten international organisations (such as the Commonwealth Secretariat, European Union, INTERPOL, the International Telecommunication Union, the Organisation of American States, the UN Office on Drugs and Crime and others), participate as members or observers in the Cybercrime Convention Committee. This Committee assesses implementation of the Convention by the Parties, and keeps the Convention up-to-date. Current efforts focus on solutions regarding law enforcement access to electronic evidence on cloud servers.

Capacity building

The value of capacity building in relation to cybercrime and -security is not a new discovery. International calls for technical assistance to reinforce criminal justice capacities on cybercrime have been made for decades. Following adoption of the Budapest Convention on Cybercrime in 2001, the Council of Europe began to assist countries in the implementation of this treaty, first within Europe and from 2006 also in other regions of the world, often in cooperation with the European Union.

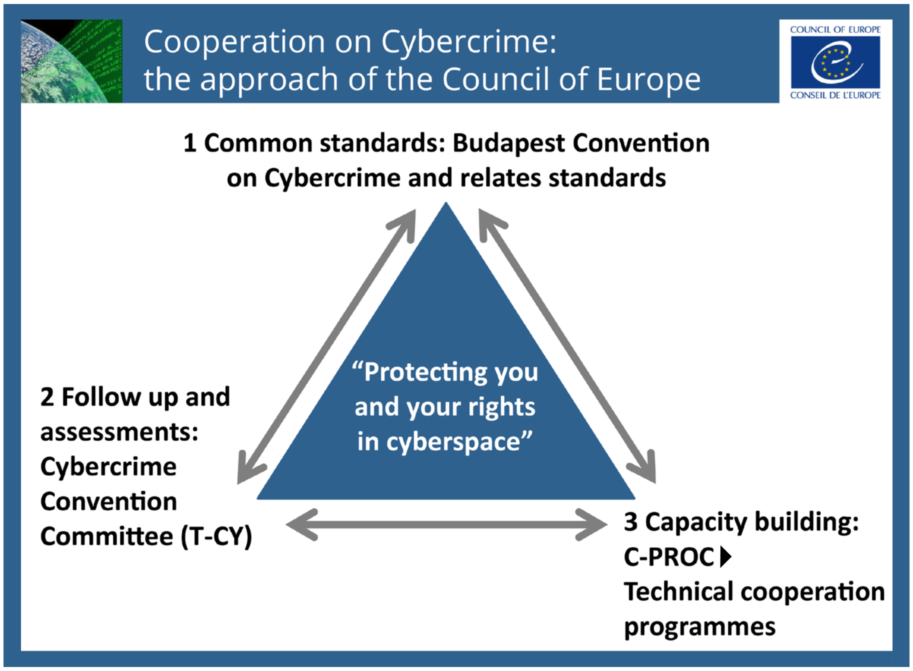
However, the year 2013 brought the matter to yet another level. The need for a broad agreement on capacity building was stated in February 2013 by the United Nations Intergovernmental Expert Group on Cybercrime and by the European Union in its Cybersecurity Strategy.

In October 2013, it was the focus of the Global Cyber Space Conference in Seoul, Korea. Building on this momentum, the the European Union and the Council of Europe followed by up immediately and in the very same week signed their agreement on the joint project on 'Global Action on Cybercrime' (GLACY), while at the same time, the Council of Europe decided to establish a Cybercrime Programme Office (C-PROC) for worldwide capacity building in Bucharest, Romania.

The creation – at the subsequent Global Cyber Space Conference (Netherlands, April 2015) – of the Global Forum on Cyber Expertise was a further logical consequence.

By August 2016, C-PROC managed a series of projects – including several joint projects with the European Union – covering the Eastern Partnership region (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) or South-Eastern Europe and Turkey (the project 'iPROCEEDS' is targeting proceeds from crime online).

With a broader geographical scope, the 'Global Action on Cybercrime' project (GLACY) assists Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga. These are priority countries given their political commitment to implement the Budapest Convention. With GLACY ending in October 2016, several of these countries will be able to share their experience within their respective regions by serving as hubs under the new joint EU-CoE project 'Global Action on Cybercrime Extended' (GLACY+), which runs from 2016 to 2020.



Cooperation on Cybercrime:
the approach of the Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

"Protecting you and your rights in cyberspace"

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Conclusion

Experience in recent years has shown that capacity building indeed is an effective way to help societies meet the challenge of cybercrime.

In general terms, political commitment, reference to common international standards and continuous participation in international peer reviews enhance the chances of success of capacity building programmes. Each project or organisation may have its own formula to make this work.

For the Council of Europe, the Budapest Convention, the Cybercrime Convention Committee and capacity building by C-PROC form a "dynamic triangle": Capacity building programmes support the implementation of the Budapest Convention as well as recommendations of the Cybercrime Convention Committee; and at the same time, the experience of capacity building programmes is fed back into the Committee and the further evolution of the Convention. The long-term involvement of "project countries" in the Cybercrime Convention Committee helps sustain the process beyond the life cycle of individual projects.

More information:

Council of Europe/Global Project on Cybercrime 2013: Capacity building on cybercrime

Council of Europe/European Union: GLACY project on Global Action on Cybercrime

Council of Europe website on cybercrime

Interview with Lynn St. Amour Chair of the Internet Governance Forum Multi-stakeholder Advisory Group

A decade of IGF: achievements and challenges ahead

“Cyber capacity Building at all levels continues to be a major challenge in the global south”

In March 2016 Lynn St. Amour was appointed as the new Chair of the Multi-stakeholder Advisory Group of the Internet Governance Forum. The Multi-stakeholder Advisory Group advises the Secretary-General on the programme of Internet Governance Forum meetings. It comprises 55 members drawn from Governments, the private sector and civil society, including representatives of the academic and technical communities. St Amour is the first Chair who does not represent the government and also the first female in this position.

Q: Looking back since the IGF was established in 2005, what has been achieved?

“The IGF has evolved over the last decade in response to community needs – and it is still true to its roots as

“The IGF has a special responsibility to increase participation in global Internet governance processes”

a forum for multi-stakeholder policy dialogue. Following this multi-stakeholder approach the IGF has delivered some tangible outputs such as the IGF Best Practice Forums (BPFs) and their reports, and the ‘Policy Options for Connecting and Enabling the Next Billion’ (CENB) project. The IGF community has grown tremendously and continues to bring in new stakeholders from across the globe. There are now over 60 National and Regional IGF Initiatives (NRIs). Annual meetings have evolved from including 30 workshops in the first years of the IGF to more than one hundred today.”

Q: How do you see the internet developing in the next decade?

“The Internet will become more mobile centric, and will become increasingly diverse and rich as the remaining 50% of the world comes online. The advances being made in connecting virtually every device to the Internet (the “Internet of Things”) means vastly more data will be collected and available. Growing acceptance of blockchain technologies and appreciation for what they can enable means they will have impact beyond financial markets.”

Q: How is the IGF going to respond to these challenges?

“In the IGF, we are working to support the World Summit on the Information Society (WSIS) vision “to build a people-centred, inclusive and development-oriented information Society”, respecting fully the Universal Declaration of Human Rights. It is anticipated that the IGF community will continue to support a continuous set of topical inter-sessional community-led activities. The IGF will make a meaningful contribution to a number of the Sustainable Development Goals (SDGs), especially the objective in Goal 9 to ‘build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation’.

Certainly, security and privacy will remain key topics for the IGF. There will continue to be challenges in the areas of security as some of the recent DDOS attacks using IoT devices such as DVR’s, etc. have shown. Security awareness is still only minimally present in most computing environments and there is a long way to go before we can impact security in such everyday items as our TVs, refrigerators, etc.”

Q: What do you regard as the main challenges in cyber capacity building, especially in the global south?

“Capacity Building at all levels continues to be a major challenge in the global south. While cyber security capacity building continues to be a challenge in virtually all countries, additional barriers exist in the form of economic and infrastructural challenges as well as in digital literacy. The IGF has a special responsibility to increase participation in global Internet governance processes, and could contribute to or lead related capacity building initiatives in this area.”

More information:

IGF Best Practice Forums (BPFs)

National and Regional IGF Initiatives (NRIs)

Meridian Conference 2016: Protecting critical information infrastructure across the world

From 7 to 10 November 2016 the Meridian community held its 11th annual conference in Mexico City. The Theme of this year's conference was 'Capability Development in Critical Information Infrastructure Protection (CIIP)'. The Meridian community actively reaches out to new countries with less developed CIIP capabilities by organizing an Introductory Day to the conference in which CIIP concepts and terminology will be introduced. This introductory day is organized in partnership with the Global Forum on Cyber Expertise (GFCE).

Written by: Peter Burnett, GFCE-Meridian Coordinator

11 years of Meridian

In 2005 a low-key governments-only conference was held in a former Naval College in the area of London known as Greenwich, near the observatory where the Greenwich Meridian was established setting the baseline for all lines of Longitude and the world's time zones. The delegates came from 30 + countries of the EU and the G8 and they talked freely about policy matters relating to CIIP. It was a fairly new subject for many of the countries, though it is now familiar to all of them and considered part of Cyber Security (which hadn't really been invented then). We called it the conference Meridian.

The event was considered very valuable and its unique format and atmosphere led to it being replicated every year since then, each time hosted by a different country. These hosts now make up the Meridian Steering Committee which governs the Meridian principles, and they agreed to try and bring the conference to new global regions each year in order to attract new countries to join this select community. It started to become evident after the first 10 years that although there is great value in an event which brings together government officials to discuss CIIP issues in a confidential environment, the nature of CIIP (all CIIs are ultimately connected and therefore weak links threaten everyone) mandates that this expertise and experience should be shared with all countries regardless of the sophistication of their CIIs. The focus has therefore shifted recently towards Capability Development, which is a new term encompassing Capacity Building as well as developing more advanced capabilities.

MERIDIAN
CONNECTING & PROTECTING
MEXICO 2016

CIIP
Capability Development
12th Meridian Conference
8th to 10th November
Primer Day 7th November

GFCE
Global Forum on Cyber Expertise

Meridian Conference 2016 in Mexico

Engaging the global south

It is one thing to have a policy stating that Meridian is open to all countries, but quite another to attract many of those who are not yet fully engaged in CIIP or who simply lack the political awareness or resources to send any delegates. Furthermore, attending a well-established event like this and mingling with many of the world's leading policy experts can seem a daunting prospect for someone new to the subject. We have therefore established a special Introductory Day this year immediately before the main conference, in order to explain the concepts, terminology, developments and to introduce some of the key global organisations in the field. We are hoping that this will not only attract new countries to the Meridian but help their delegates to get the most out of the event. The aim is to establish close and trusting relationships with a wide range of other countries that are all focussed on the same issues.

Following through on the Introductory Day, a Buddying programme was launched during Meridian 2016 in which new members can partner with established Meridian members. The idea is to buddy countries based on shared mutual interests, either between peer countries, developed and developing partners, or any other combination. The Buddying programme is intended to facilitate the sharing of the pool of experience, knowledge and ideas that is unique to Meridian and help everyone reach an optimum level of CIIP and be prepared for the ever-increasing challenges that threaten this increasingly vital aspect of a nation's infrastructure.

Meridian – GFCE Initiative

The Meridian has no resources of its own and relies on funding by individual members (such as hosting of annual conferences, the website and secretarial services). For its capacity building activities and outreach, Meridian has partnered with the GFCE. More information about the GFCE-Meridian initiative on Critical Information Infrastructure Protection is available on the GFCE website. New members of the Meridian receive access to the CIIP directory on the Meridian website with valuable resources (including contacts on CIIP related matters).

GFCE Annual Meeting 2016: Connecting the dots in global cyber capacity building

During the first Annual Meeting of the Global Forum on Cyber Expertise (GFCE) in June 2016 over 100 cyber policymakers and stakeholders from all over the world met in Washington D.C. It was a first opportunity to present the results of the current 12 cyber capacity building initiatives under the GFCE umbrella. The meeting was deliberately organized as a market place to exchange experiences, learn about global best practices and network with valuable organizations both in and outside the GFCE community.

Written by: GFCE Secretariat

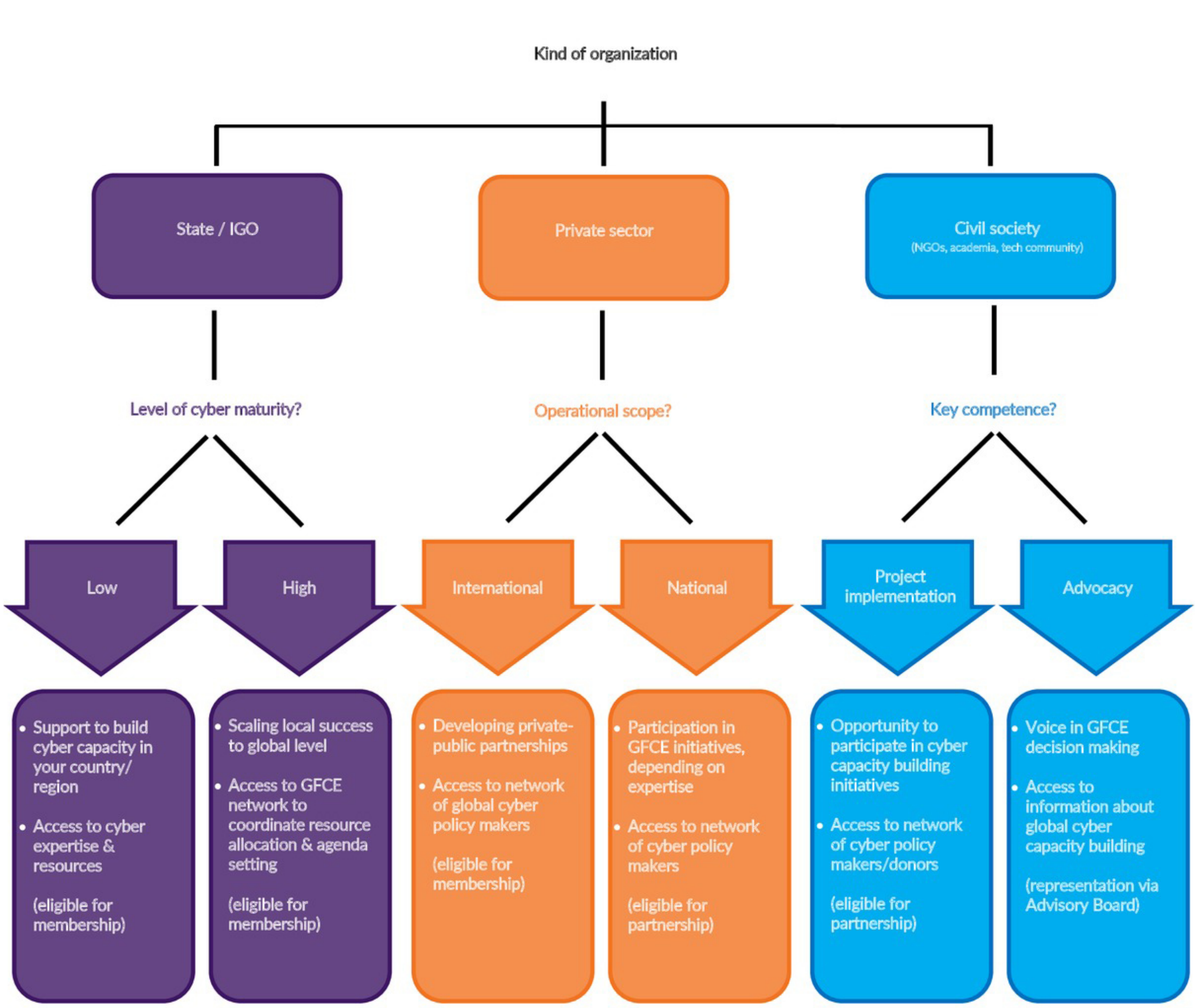
Open platform

During the Annual Meeting it became once more apparent how much is already happening in cyber capacity building. Different GFCE members and invitees presented their cyber capacity building projects and initiatives in 17 working sessions. Session discussions demonstrated the very similar challenges organizations all around the world are facing on topics such as developing Cyber Strategies and Computer Emergency Response Teams (CERT), assessing cyber threats, raising cyber campaigns, implementing legal frameworks and workforce training.

While a lot is happening in cyber capacity building, especially in bilateral and regional cooperation, there is also a lack of overview and mechanisms for multistakeholder cooperation on a global level. This is where the GFCE proves its added value. The GFCE aims to provide an overview of worldwide activities and actors in cyber capacity building. Members in the process of building up their cyber capacity can take full advantage of the GFCE network to attract expertise and donors for their cyber capacity building ambitions. More experienced members benefit by sharing lessons learned and scaling local best practices to a global level. The GFCE is an open platform, which means it is open for partnerships and cooperation with external stakeholders. During the Annual Meeting different relevant external stakeholders where invited to share their experiences and best practices, such

> “The GFCE aims to provide an overview of worldwide activities and actors in cyber capacity building.”

How your organization can benefit from the GFCE network



Kind of organization

State / IGO

Level of cyber maturity?

Low

- Support to build cyber capacity in your country/ region
- Access to cyber expertise & resources

(eligible for membership)

High

- Scaling local success to global level
- Access to GFCE network to coordinate resource allocation & agenda setting

(eligible for membership)

Private sector

Operational scope?

International

- Developing private-public partnerships
- Access to network of global cyber policy makers

(eligible for membership)

National

- Participation in GFCE initiatives, depending on expertise
- Access to network of cyber policy makers

(eligible for partnership)

Civil society (NGOs, academia, tech community)

Key competence?

Project implementation

- Opportunity to participate in cyber capacity building initiatives
- Access to network of cyber policy makers/donors

(eligible for partnership)

Advocacy

- Voice in GFCE decision making
- Access to information about global cyber capacity building

(representation via Advisory Board)

Want to know more? contact@thegfce.com or visit thegfce.com

as the World Economic Forum (WEF), the World Bank and Diplofoundation.

Multistakeholder involvement

During the Annual Meeting a step forward was also made to include civil society in the work of the GFCE. Nine civil society representatives were selected based on an open call for application to form the GFCE Advisory Board. The Board was formally established during the Annual Meeting with the mandate to advice GFCE members and initiatives both on request and on their own initiative. The Advisory Board will play an important role in future Annual Meetings and GFCE decision–making process.

Through membership by states and regional intergovernmental organizations, the GFCE currently represents 66% of the world population. The multistakeholder approach of the GFCE is reflected in openness for members- and partnership for the private sector, NGOs and the Advisory Board. This comprehensive representation of cyber policymakers and stakeholders in the GFCE provides opportunities for future coordination and agenda setting in cyber capacity building.

Volume 2, November 2016
Global Cyber Expertise Magazine

Colophon

Editorial board	Anne Blanksma Çeta (GFCE) Belisario Contreras (OAS) Panagiota-Nayia Barmpaliou (EU) Souhila Amazouz (AU)
Guest editors	Alison August Treppel Folake Olagunju Oyalola Kaleem Ahmed Usmani Jennita Rao Appanah Jairo Hernan Marin Agudelo Juan Carlos Buritica Grajales Carlos Andrés Arbelaez Velasquez Peter Burnett Renato Opice Blum Gerard Hartsink
Artwork & design	Ivonne Vivanco (OAS)
Chief editor (rotating)	Barbara Marchiori de Assis (OAS) Kerry-Ann Barrett (OAS)

Publishers

African Union, www.au.int,
contact@africa-union.org, @_AfricanUnion

European Union, www.europa.eu,
SECPOL-3@eeas.europa.eu, @EU_Commission

Global Forum on Cyber Expertise,www.thegfce.com,
contact@thegfce.com, @thegfce

Organization of American States, www.oas.org/cyber,
cybersecutiry@oas.org, @OEA_Cyber

Disclaimer

The opinions expressed in this publication are solely those of the authors and do not necessarily reflect the views of the AU, EU, GFCE or OAS or the countries they comprise of.

Global Cyber Expertise Magazine
AU | EU | GFCE | OAS
contact@thegfce.com

Deadline submissions issue 3:
February 1st, 2017