2018

White paper series
Issue 3

OPPORTUNITIES AND CHALLENGES FOR SMES IN THE CONTEXT OF INCREASED ADOPTION OF ICTS

OAS | More rights for more people | aws

OPPORTUNITIES AND CHALLENGES FOR SMES IN THE CONTEXT OF INCREASED ADOPTION OF ICTS

CREDITS

Luis Almagro

Secretary General
Organization of American States (OAS)

OAS Technical Team

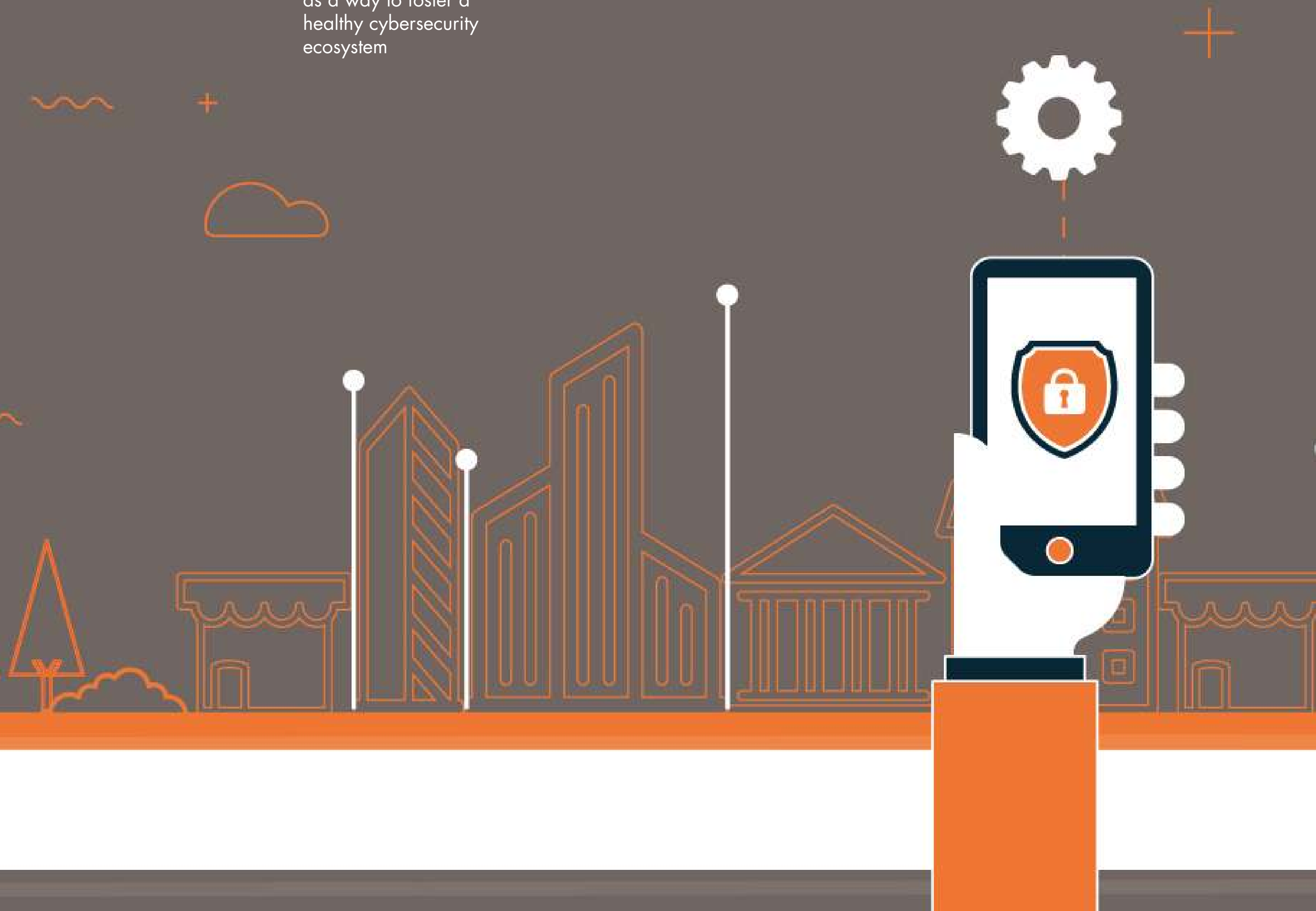
Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Nathalia Foditsch
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Gonzalo García-Belenguer
Mariana Cardona

AWS Technical Team

Min Hyun
Michael South
Maria Saab

OPPORTUNITIES AND CHALLENGES FOR SMES IN THE CONTEXT OF INCREASED ADOPTION OF ICTS

CONTENT



OPPORTUNITIES AND CHALLENGES FOR SMES IN THE CONTEXT OF INCREASED ADOPTION OF ICTS

Executive Summary

Companies from different sizes and in different sectors are increasingly relying on Information and Communication Technologies (ICTs), and this has been key to innovation, productivity and growth. Despite the countless benefits and opportunities, there are challenges that arise when adopting ICTs, and small and medium enterprises (SMEs), generally face higher challenges if compared to larger companies. Having a poor ICT infrastructure, not knowing how to properly address complex cybersecurity threats, or underestimating the importance of protecting personal data are examples of these challenges faced by SMEs. Thiswhite paper therefore briefly describes some of the difficulties faced by SMEs given the increased adoption of ICTs. It also addresses crucial considerations pertaining to personal data protection and privacy, and the importance of making some institutional changes that allow for a "security-aware" culture to be created. It also explains how governments play different roles as enablers of a healthy ecosystem, such as when procurement rules are used as a means to foster the adoption of cybersecurity standards, or when capacity building efforts directed to SMEs are promoted. Lastly, a few straightforward steps that can be taken by SMEs when looking at strengthening their cybersecurity preparedness are outlined in the penultimate paragraphs..

OPPORTUNITIES AND CHALLENGES FOR SMES IN THE CONTEXT OF INCREASED ADOPTION OF ICTS

1

Small and medium enterprises (SMEs) are found everywhere in the Americas. They are your neighborhood bakery, the family-owned bike-shop, the local Internet provider and software designing company. They are well-known for their positive impact in societies and are considered "essential for delivering more inclusive globalization and growth" (OECD, 2017, p.5) as they have demonstrated to be fundamental for the social and economic development of countries. "Startups", organizations "formed to search for a repeatable and scalable business model" (Blank, 2010), have also become popular across the Americas over the years. [1]While the contributions of such enterprises might vary across enterprises, countries and sectors, different studies suggest that they are indeed fundamental in alleviating poverty and creating jobs (E.g. Deijl et al., 2013; Lopez-Acevedo & Tan, 2011).

This increased role of the SMEs is to a large extent supported by their growing reliance on the Internet and Information and Communication Technologies (ICTs), which allow them to take advantage of the global economy, as well as to strengthen processes, efficiency, and to innovate. Indeed, startups largely rely on ICTs, representing new models of knowledge creation, innovation and promoting an entrepreneurial culture. Startups in Latin America, for example, have attracted investments that have more than doubled over the past five years, although these numbers are still lower than the ones found in other global emerging regions (Ruvolo, 2018). One example of the growth of ICT use by such organizations is the rampant increase in new financial technologies (Fintech) start-ups in Latin American and Caribbean countries[2] over the past years and there are actually hundreds of them in the region, making use of online platforms and boosting other SMEs' access to credit (IDB and Finnovista, 2017).[3]

Despite such increased role, SMEs face specific challenges compared to larger companies, such as more obstacles to innovation and access to research networks and patenting schemes (Zuniga et al., 2016). Challenges related to accessing financial instruments have also been raised in different studies (OECD, 2017; Zuniga et al., 2016). Indeed, poor "ICT infrastructure prevents SMEs from operating efficiently and accessing international markets at competitive costs" (OECD, 2017, p. 12). But it is not only the competitiveness and efficiency that is affected when the right infrastructure, skills and governance are not in place. The issue of security is also a major one and has gained a lot of attention over the past years as cyber-attacks to SMEs have been prevalent. SMEs might face losses with larger costs per capita if compared to larger enterprises and many SMEs are not yet knowledgeable about how to tackle the issue (Zec & Kajtazi, 2015).

[1] While SMEs and startups are not the same, having differences such as funding methods and scability, both models are smaller than the larger companies and might have similar challenges related to cybersecurity, data privacy and protection. Thus, the term "SMEs" is used interchangeably in this document.

[2] Examples of popular Fintech segments are "alternative finance platforms"; "payment solutions"; "enterprise financial management"; and "personal financial Management", and Brazil, Mexico, Argentina, Colombia and Chile are the countries within the region with most Fintech companies (IDB and Finnovista, 2017).

[3] As noted by Cathles (2014), there is a lack of "timely entrepreneurship indicators on business demographics" (p.22) in Latin American and Caribbean countries, as only "partial information about entrepreneurship" (p. 24) in the region can be found.

Over the years the challenges faced by companies in combating cyber risks have changed as the types of risks have evolved. In the first decade of the 2000's, organizations dealt with challenges such as spyware and "automated phishing" detection as well as the detection of proxy bypass websites, but more complex challenges such as "spear phishing detection" are now common (Symantec, 2018). Advanced threats such as "ransomware" are even able to "infect the organization and log clean-up mechanisms to cover their tracks" (Bitdefender, 2017, p.2). Indeed, according to PwC (2018), the main worry of CEOs in the United States is facing cyber threats.

Besides the increased complexity of the threats, cybersecurity should be seen from different dimensions. A wide variety of definitions of cybersecurity have been created, although many of these definitions are not holistic or interdisciplinary as they should be (Craigen et al., 2014). As briefly explained below, the understanding of cybersecurity has evolved over the years, and now entails more than purely technical activities and breaches but also different types of unauthorized exploitations and uses of data.[4] Indeed, data privacy and personal data protection are also parts of the challenge for most types of businesses.

[4] Different regulatory frameworks treat "personal data" differently than other types of data. While the concept has not been applied equally across countries, it generally refers to data that allows a person to be personally identified.

SMES, DATA PRIVACY AND PERSONAL DATA PROTECTION

2

Since the 2013 revelations of international surveillance activities in foreign countries,[5] several countries in the region have started to discuss or to create legal and policy frameworks aimed at protecting personal data and privacy, and the awareness related to cyber risks has increased (Maciel et al., 2016). Security can thus be understood more broadly, also encompassing data protection related aspects, and SMEs should understand how data should be collected, stored, mined, used and protected.

Legislation related to privacy and personal data protection is not new to the Americas, and has existed in different countries in the region for over thirty years (Cerda, 2012). However, there are different frameworks in place, with different levels of maturity. For example, most countries in the Americas do not have a personal data protection authority, and the only countries in the Americas which are signatories of the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" are Argentina, Mexico and Uruguay.[6] Given such a scenario, there is no minimum level of data protection or privacy standards that have to be guaranteed across all countries in the Americas. This does not mean, however, that SMEs should not take the protection of personal data and privacy seriously, nor to a larger extent cybersecurity,. Indeed, by providing a solid level of protection, SMEs create a competitive advantages and trust is strengthened. In fact, not only trust might be affected by a poor management of personal data protection and privacy but even the sales cycle could be affected or financial losses in the case of a breach, might occur. According to CISCO (2018) the sales cycle of companies can be deeply affected due to consumer data privacy concerns. "Privacy mature" organizations, in turn, are less likely to face delays in their sales cycle, or data breaches losses. Moreover, companies with a hybrid privacy organizational model (compared to a centralized or decentralized models) were found to be less likely to face sales delays (CISCO, 2018). As we can see, SMEs should also attempt to create a governance model that leads to positive impacts on cybersecurity related topics.

Besides the company's governance, products and services themselves can be designed so that protections are in place "by design", a broad concept that involves different aspects, as explained in the box below.

[5] These revelations showed that the United States had surveilled foreign countries. Indeed, the revelations showed that "National Security Agency (NSA) and other U.S. law enforcement and national security agencies have used provisions in the Foreign Intelligence Surveillance Act (FISA) and USA PATRIOT Act to obtain electronic data from third parties" (Castro, 2013, p. 1). Clarke et al (2013) argued that "foreign concerns about US surveillance can directly reduce the market share of US-based technology companies, and can in addition have an indirect effect of justifying protectionist measures" (p. 212).

[6] See "Chart of signatures and ratifications of Treaty 108", available at www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=wWwV2sLp

BOX #1 Privacy by Design

The concept of "privacy by design" has existed for several years and it is key to data security. It generally refers to "embedding privacy into information technologies, business practices, and networked infrastructures, as a core functionality, right from the outset – means building in privacy right up front – intentionally, with forethought" (Cavoukian, 2012, p. 39).

Business owners can operationalize this concept in different ways, including developing software that incorporates privacy requirements such as minimizing data collection, using de-identification processes, or employing "encryption by default"[7] (Cavoukian, 2012). Because of the large amounts of data that SMEs might collect, mine and store data, the challenge of implementing privacy protections is more important than ever, but also more difficult than ever. For example, several business models rely on "big data" and "digital breadcrumbs left behind by individual's use of technologies and later repurposed for analysis" (D'Acquisto et al., 2015, p.22). For this reason, minimizing data collection and protecting personal data while allowing data to be transformed, mined and analyzed in ways that are useful and valuable for the private and public sectors is a major challenge.

Some regulatory frameworks expressly contain rules related to "privacy by design". The General Data Protection Regulation (GDPR), for example, which has entered into force in the European Union in 2018, has established expectations on "privacy by design" and also claims that "by default, only personal data which are necessary for each specific purpose of the processing" should be processed.[8] Indeed, such requirements will have to be followed when companies are entering public contracts, as described further in this document.

Despite the fact that increasing cybersecurity and privacy protections have become progressively important steps over the past years, not all SMEs are fully aware of the benefits of implementing them, or sometimes lack resources and capabilities to doing so.

[7] Check New America Foundation's " Using Encryption by Default" Case Study, available at https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-1-using-transit-encryption-default/

[8] Article 25 (2), GDPR: "The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. 3In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

SMES AND CYBERSECURITY AWARENESS

3

The level of awareness and readiness in regard to cybersecurity and privacy varies widely depending on the SME. While some might have understood and applied steps towards protecting their resources and implemented capabilities, some of them might not yet have any in place. Indeed, part of this problem is due to the lack of "security culture", defined as "attitudes, beliefs and perceptions shared by the members of the group, who define norms and values which, in turn, determine the way they act and react regarding risk and the risk control system" (Lopes and Oliveira, 2014, p. 278). The lack of a security culture might lead to a limited understanding of security among SMEs, which tend to implement measures that protect the physical and logical layers of their networks but underestimate the human component, such astraining employees and monitoring compliance (Lopes and Oliveira, 2014)

If strengthening the security culture withing SMEs is needed, what should be done about it? One important issue is certainly to raise awareness and to provide training to employees. Beyer et. al. (2015[9] argue that "security is currently not part of the psychological contracts in most organizations" (p.8) and explain some of the key points related to awareness campaigns, such as the removal of security tasks that are unrealistic, the focus on achieving behavioral changes, and getting employees progressively involved. The human aspect of cybersecurity should not, thus, be underestimated, and these are some of the ways it can be strengthened. One empirical study that tried understanding the organizational, technological and psychological aspects of cybersecurity in SMEs found that a large majority of the employees (two-thirds) did not report their mistakes to their superiors (Zec & Kajtazi, 2015). Moreover, the "absence of internal cyber policies in SMEs" and the "low financial investments" were also found to be factors that put SMEs in a vulnerable position (Zec & Kajtazi, 2015, p. 237).

In another empirical study, Burgurcu et al. (2010) have found that information security can be improved if a "security-aware" culture within the organization is created, and that rewards such as recognizing "trustworthiness, reputation, and good image" (p.544) of employees that comply with security rules can positively impact the way employees perceive the benefit of such compliance, changing their behaviors and attitudes for the better. While employees perceive compliance efforts as burdensome, allocating a certain amount of their time, without disrupting their routines, to awareness and compliance efforts and simplifying procedures might mitigate such perception (Bulgurcu et al., 2010; Lopes & Oliveira, 2014). Further, technological developments that allow some of the tasks to be easily automated, something that should also be considered by SMEs when evaluating options.

According to PwC (2018), the number of board members who engage in the oversight of security and privacy risks is less than one third, a reality that is expected to change, given the fact that security

[9] While many of them might not have the intent to hide their mistakes, it seems that the human aspect of organizations is important when assessing the vulnerabilities of companies. Zec & Kajtazi (2015) also suggested that personality traits should be taken into consideration when professionals are being selected to take roles related to information security (e.g. they argue that the ones with higher "guilt proneness" should be better at maintaining the company secure)

and privacy concerns directly impact outcomes and consequently the profitability of the companies. Moreover, hiring an executive whose main duty is to be responsible for overseeing the privacy and security in the company is a trend that is now commonly found in large organizations. Indeed, two-thirds of the "Fortune 1000" companies have already assigned a "chief data officer" or "chief privacy officer", although there is "evident confusion and disagreement on the mandate and importance" of their roles (NewVantage Partners, 2018, p.8). The existence of such professional - also frequently referred to as "chief information officer" (CIO) - is not yet a widespread trend in smaller organizations (PwC, 2018), but this scenario is likely to change as more organizations become acquainted with the challenges and opportunities brought by new technologies.

As demonstrated above, each individual organization is responsible for its business as well as securing the data they amass, store and use. Notwithstanding, governments can also be instrumental in fostering a security-conducive ecosystem, and such role is briefly described below.

THE ROLE OF THE GOVERNMENT IN PROMOTING A HEALTHY CYBERSECURITY ECOSYSTEM FOR SMES

4

The private sector "acts as a laboratory for identifying, developing, and implementing cybersecurity best practices that inform domestic and international policymaking" (Shackelford et al., 2015, p.360). SMEs, while a part of this group, might not have all the technical, human and financial resources needed to get a full grasp of the cybersecurity and privacy steps they need to adopt, implement and use. There is, for this reason, a role to be played by governments across the Americas in supporting the creation of a healthy cybersecurity ecosystem for SMEs.

As shown by Mazzucato (2013), it is a mistake to assume that the state does not play a role in advancing technologies, as some of the main technology companies have largely benefited from governmental policies which were directed at allowing for risks to be taken. She highlighted the role of decentralized and "mission oriented" policies, such as the ones that led to the creation of technologies such as the Internet, the World Wide Web, cellular communication technology and the GPS were also developed with the support of public funding (Mazzucato, 2013).

The issue of security brings new challenges for governments, which are now facing the challenge of not only fostering the creation and adoption of such technologies, but also supporting a healthy ecosystem which prioritizes cybersecurity needs. Awareness raising, capacity building, and well as more direct interventions such as the establishment of minimum security rules for cybersecurity in public procurement are some of the ways this role is played, as briefly described below.

Public procurement efforts have been used as a way to foster social justice, and social change for several decades (McCrudden 2006 and 2007). One example is the growth of availability of accessible devices fostered through public procurement, what has been done in different countries such as the United States, Japan, Canada, and United Kingdom and has positively impacted persons with disabilities (Tibben & Astbrink, 2012). With cybersecurity it is not different, as some countries have already established rules directed towards assuring that public procurement respects minimum cybersecurity related requirements.

BOX #2 Public Procurement- A tool to foster a healthy cybersecurity ecosystem

The General Data Protection Regulation (GDPR), which has recently entered in to force in Europe as described above, is an example of a framework that includes rules related to government contracts involving the processing of personal data. Because of it, "government bodies will need to review and conduct due diligence on existing and future contracts under which personal data is processed" (Tucker, 2018).

In the United States, some of the regulations pertaining to cybersecurity requirements in governmental contracts have been even tested at an administrative level. The National Institute of Standards and Technology's ("NIST") has established, for example, that "security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit Controlled Unclassified Information or that provide security protection for such components", requirements that are "intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations" (SP 800-171 Rev. 1).[10] Reynolds (2018) notes that such rules have even been challenged at the administrative level, as the U.S. Government Accountability Office has issued two decisions related to the application of such rules. Indeed, it is expected that "more agencies explicitly incorporating cybersecurity requirements into solicitations" will be seen, and "offerors that fail to demonstrate full compliance may be disqualified as technically unacceptable or be downgraded for evaluation purposes" (Reynolds, 2018).

In some cases, security reasons justify the direct contracting in public procurement contracts according to the legal and regulatory frameworks in different countries in the Americas. Examples are Argentina, Bolivia, Brazil Chile Costa Rica, Guyana, Honduras, Jamaica, Panama and Peru, where security considerations are "special circumstances" that might "make holding a competitive process a practical impossibility"

[10] NIST. SP 800-171 Rev. 1 https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

(Benavides et al., 2016, p. 48). With cybersecurity it might not be different, and it is possible to predict occasions in which direct contracting of companies could be justified, as benefits of maintaining a baseline level of cybersecurity might outweigh cost reductions of products and services whichdisregard cybersecurity. While SMEs should make efforts to comply with cybersecurity standards,[11] governments should support them in taking the right steps. Public procurement rules might be developed or changed in order to offer incentives for those SMEs that chose to adopt and comply with such standards. Further, a tiered approach in which companies' with different sizes are requested to comply with different levels of cybersecurity can be developed in a way to avoid overburdening the smaller companies.

The role of the government might also entail capacity building and awareness raising efforts, a demand highlighted in a joint study published by OAS, the Inter-American Development Bank and the Colombian Ministry of Information Technology and Communication in 2017 (OAS et al., 2017), as well as policies corresponding to more direct interventions.[12] Governmental programs aimed at supporting SMEs do already exist and have proved to be valuable in supporting a favorable ecosystem to SMEs. An assessment of SME support programs in four Latin American countries (Chile, Colombia, Mexico and Peru) found statistically significant positive impacts of such programs, especially regarding to sales and firm performance (Lopez-Acevedo & Tan, 2011). For example, participating in programs directed to SMEs in Chile, such as business networking programs and export promotion programs, was found to be associated with positive improvements in the short and intermediate terms, and in Colombia, SMEs that were benefited by a governmental fund were positively impacted in regards to exports and investment in R&D (Lopez-Acevedo & Tan, 2011). Policies directed towards capacity building efforts might also entail developing content and knowledge, as well as courses and training programs that can be useful for SMEs. Such contents might be developed by public authorities alone or in partnership with private companies with expertise in cybersecurity. Capacity building and awareness raising initiatives might target, for example, developing awareness toolkits and aligning national campaigns (GFCE, 2017).[13]

The role of the government is an extensive one, as described above. Even though governments have been playing an active role and, in many cases, have served as a fundamental pillar for SMEs' success, there is still a lot to be done. Such scenario is especially true considering that the adoption of new technologies coupled with the increased amount of data collected, mined, stored and used by companies is increasing at an exponential rate.

If the scenario above described is understood, governments have the chance of not only protecting SMEs but fostering a more secure ecosystem, in which trust and economic prosperity are likely to emerge. It is possible to conclude, thus, that both private and public sectors have a role to play. Indeed, each SME should also make concrete efforts to create a secure ecosystem, and there are steps that can be taken by them in order to strengthen their cybersecurity readiness, some of which are described below.

[11] SMEs should, for example, look into the requirements established by official cybersecurity standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework; the Service Organization Control (SOC) Reports, and the International Organization for Standardization (ISO) standard for cybersecurity. Each one has different characteristics and corresponds to a different methodology.

[12] Examples of such efforts are the ones undertaken by the United States' Department of Homeland Security, such as the " National Cyber Security Awareness Month" , which "is an annual campaign to raise awareness about the importance of cybersecurity". The STOP. THINK. CONNECT.™ is another awareness raising efforts that is led by a coalition of public and private stakeholders as well as NGOs aimed at helping "people understand not only the risks that come with using the Internet, but also the importance of practicing safe online behavior" . See more information at https://www.dhs.gov/national-cyber-security-awareness-month and at www.stopthinkconnect.org/.

[13] The 2017 "Global Agenda for Cyber Capacity Building" developed by the Global Forum on Cyber Expertise (GFCE) has identified different initiatives related to capacity building and awareness raising (GFCE, 2017)

ACTIVE MEASURES THAT CAN BE TAKEN BY SMES IN ORDER TO STRENGTHEN THEIR CYBERSECURITY

5

Considering the challenges and opportunities outlined above, there are different measures that can be taken by SMEs willing to strengthen their cybersecurity preparedness. The list below provides guidance over what some of these important measures are:

1. **Select one employee to be in charge of all cybersecurity and data protection and privacy related aspects.**
   This person should be fully dedicated to these tasks, if possible. If such commitment is not possible due to budgetary constraints, ensure that one person is responsible at least in a part-time basis and provide them adequate training. One important factor is to select a person with adequate skills and personality, as the role demands careful attention and knowledge;

2. **Create a "security-aware" culture within your SME.**
   Internal policies, awareness campaigns and capacity building programs are some of the ways to achieve this goal. Different programs can be created for different types of employees, but all of them should have a minimum level of awareness of issues pertaining the importance of cybersecurity. Moreover, avoid disrupting or overburdening employees and give them plenty of time to take such training sessions;

3. **Design products and services with embedded privacy and personal data protection.**
   (read about the "privacy by design" and "privacy by default" concepts above). This is not only a socially responsible practice but helps to avoid potential security and privacy related liability. Further, companies that have such designs embedded in their core businesses have competitive advantages that might pay off;

4. **Look for available resources, especially governmental efforts directed towards supporting SMEs**. Moreover, there are plenty of resources available online to be carefully studied. Given the nature of the topic, a constant effort to update knowledge and skills is necessary;

5. **Comply with official cybersecurity and data protection standards and public procurement requirement**s. If such requirements do not exist, communicate to policy makers and legislators that they should be implemented. It is everyone's interest to have a healthy and secure business and governmental ecosystem.

REFERENCES 6

- Benavides, J. L., M'Causland Sánchez, M. C., Flórez Salazar, C., & Roca, M. E. (2016). Public Procurement in Latin America and the Caribbean and IDB-financed Projects - A Normative and Comparative Study. Inter-American Development Bank.

- Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. A framework for progressive engagement of staff in cyber security. Retrieved from https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

- Bitdefender. (2017). The Global Threat Landscape Report - 2017. Retrieved from https://download.bitdefender.com/resources/files/News/CaseStudies/study/181/Bitdefender-Business-2017-Whitepaper-threat-landscape-crea2186-en-EN-GenericUse.pdf

- Blank, S. (2010). What's A Startup? First Principles. Retrieved April 3, 2018, from https://steveblank.com/2010/01/25/whats-a-startup-first-principles/

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34, 523–548.

- Castro, D. (2013). How Much Will PRISM Cost the U.S. Cloud Computing Industry? (p. 9). ITIF. Retrieved from http://www2.itif.org/2013-cloud-computing-costs.pdf

- Cathles, A. (2014). Entrepreneurship Data for Latin America and the Caribbean -What Is There and What Is Missing? Inter-American Development Bank. Retrieved from https://publications.iadb.org/bitstream/handle/11319/6744/CTI_TN_Enterpreneurship_Data_for_Latin_America_and_the_Caribbean.pdf

- Cavoukian, A. (2012). Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Information and Privacy Commissioner of Ontario. Retrieved from http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf

- Cerda Silva, A. (2012). Protección de datos personales y prestación de servicios en línea en América Latina. In Hacia una Internet Libre de Censura: propuestas para América Latina I (Eduardo Bertoni). Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo. Retrieved from http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

- CISCO. (2018). Privacy Maturity Benchmark Study. CISCO. Retrieved from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-maturity-benchmark-study-2018.pdf
- Clarke, R., Morell, M., Stone, G., Sunstein, C., & Swire, P. (2013). Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. White House Review Group on Intelligence and Communications Technologies. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

- Cook, K. (2017). Effective Cyber Security Strategies for Small Businesses. Walden Dissertations and Doctoral Studies. Retrieved from http://scholarworks.waldenu.edu/dissertations/3871

- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, (4(10)), 13–21.

- D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., Montjoye, Y.-A. de, & Bourka, A. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. European Union Agency For Network And Information Security (ENISA).

- Deijl, C., de Kok, J., & Veldhuis-Van Essen, C. (2013). Is Small Still Beautiful? Literature Review of Recent Empirical Evidence on the Contribution of SMEs to Employment Creation. Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. Retrieved from http://lup.lub.lu.se/record/cfac576e-a5c4-4802-b5f3-7989d9bffd46

- GFCE. (2017). Global Agenda for Cyber Capacity Building. Retrieved from https://www.thegfce.com/documents/publications/2017/11/20/gfce-global-agenda

- IDB, & Finnovista. (2017). Fintech: Innovations you may not know were from Latin America and the Caribbean. Inter-American Development Bank and Finnovista. Retrieved from https://publications.iadb.org/bitstream/handle/11319/8265/FINTECH-Innovations-You-May-Not-Know-are-from-latin-America-and-the-Caribbean.pdf?sequence=7&isAllowed=y

- Lopes, I., Oliveira, P. (2014). Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. In. Rocha Á., Correia A., Tan F., Stroetmann K. (eds) New Perspectives in Information Systems and Technologies, Volume 1. Advances in Intelligent Systems and Computing, vol 275. Springer, Cham . Lopez-Acevedo, G., & Tan, H. W. (2011). Impact evaluation of small and medium enterprise programs in Latin America and the Caribbean (No. 61641) (pp. 1–146). The World Bank. Retrieved from http://documents.worldbank.org/curated/en/587801468183890334/Impact-evaluation-of-small-and-medium-enterprise-programs-in-Latin-America-and-the-Caribbean

- Maciel, M., Foditsch, N., Belli, L., & Castellon, N. (2016). Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean. In 2016 Cybersecurity Report. OAS / IDB.

- Mazzucato, M. (2013). The Entrepreneurial State: Debunking Public vs. Private Sector Myths. Anthem.

- McCrudden, C. (2006). Corporate Social Responsibility and Public Procurement (SSRN Scholarly Paper). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=899686

- McCrudden, C. (2007). Buying Social Justice: Equality, Government Procurement, and Legal Change. Oxford University Press. Retrieved from http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199232420.001.0001/acprof-9780199232420

- NewVantage Partners, (NVP). (2018). Big Data Executive Survey 2018 - Executive Summary of Findings. Retrieved from http://newvantage.com/wp-content/uploads/2018/01/Big-Data-Executive-Survey-2018-Findings-1.pdf

- OAS, IDB, & MINTIC. (2017). Impact of Digital Security Incidents in Colombia 2017. Retrieved from http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

- OECD. (2017a). Active with Latin America and the Caribbean. Retrieved from http://www.oecd.org/global-relations/Active-with-Latin-America-and-the-Caribbean.pdf

- OECD. (2017b). Enhancing the Contributions of SMEs in a Global and Digitalised Economy (Meeting of the OECD Council at Ministerial Level). Paris. Retrieved from https://www.oecd.org/mcm/documents/C-MIN-2017-8-EN.pdf

- PwC. (2018). Revitalizing privacy and trust in a data-driven world - Key findings from The Global State of Information Security Survey 2018 (p. 23). Retrieved from https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

- Reynolds, T. (2018, January). Top Five Government Contractor Cybersecurity Considerations for 2018. Retrieved from http://govcon.mofo.com/defense/top-five-government-contractor-cybersecurity-considerations-for-2018/

- Ruvolo, J. (2018, February 28). Global tech firms and investors are reshaping Latin America's startup environment. TechCrunch. Retrieved from http://social.techcrunch.com/2018/02/27/global-tech-firms-and-investors-are-reshaping-latin-americas-startup-environment/

- Shackelford, S., Fort, T. L., & Prenkert, J. D. (2015). How Businesses Can Promote Cyber Peace. University of Pennsylvania Journal of International Law, 36(2). https://doi.org/10.2139/ssrn.2393528

- Symantec. (2018). Rethinking Security for the Cloud GenerationWelcome to the Cloud Generation. Retrieved from https://www.symantec.com/theme/cloud-generation

- Tibben, W., & Astbrink, G. (2012). Government ICT Purchasing: What differences do accessibility criteria make for people with disabilities? University of Wollongong and GSA Information Consultants. Retrieved from http://accan.org.au/index.php?option=com_content&view=article&id=495:government-ict-purchasing-what-differences-do-accessibility-criteria-make-for-people-with-disabilities&catid=98:acces-s-for-all&Itemid=234

- Tucker, I. (2018, January). Government procurement prepares for GDPR. Retrieved from https://www.lexology.com/library/detail.aspx?g=4cbf7ab3-2082-44d3-a41e-f2edc4537d48

- Zec, M., & Kajtazi, M. (2015). Examining how IT Professionals in SMEs Take Decisions About Implementing Cyber Security Strategy. In The European Conference on Information Systems Management; Reading (pp. 231–239). Reading, United Kingdom, Reading: Academic Conferences International Limited. Retrieved from https://search-proquest-com.proxyau.wrlc.org/docview/1776778140/abstract/1F1546EA8CF452FPQ/1

- Zuniga, P., Negri, F. de, Dutz, M., & Rauen, A. (2016). Conditions for Innovation in Brazil: a review of key issues and policy challenges. IPEA, (218), 110.

OPPORTUNITIES AND CHALLENGES FOR SMES IN THE CONTEXT OF INCREASED ADOPTION OF ICTS

OPPORTUNITIES AND CHALLENGES — FOR **SMES** IN THE — CONTEXT OF INCREASED ADOPTION OF ICTS

OAS More rights for more people | aws

White paper series
Issue 3

2018