NIC.br
Sectoral Studies

DIGITAL SECURITY:

An analysis of risk management in Brazilian enterprises

nic.br

Brazilian Network Information Center

Brazilian Network
Information Center – NIC.br

NIC.br
Sectoral Studies

DIGITAL SECURITY:
An analysis of risk management
in Brazilian companies

Brazilian Internet Steering Committee – CGI.br
São Paulo 2020

Brazilian Network Information Center – NIC.br
CEO
Demi Getschko

CFO
Ricardo Narchi

CTO
Frederico Neves

DIRECTOR OF SPECIAL PROJECTS AND DEVELOPMENT
Milton Kaoru Kashiwakura

CHIEF ADVISORY OFFICER TO CGI.br
Hartmut Richard Glaser

REGIONAL CENTER FOR STUDIES ON THE DEVELOPMENT OF THE INFORMATION SOCIETY – Cetic.br
MANAGEMENT: Alexandre F. Barbosa
SECTORAL STUDIES AND QUALITATIVE METHODS COORDINATION: Tatiana Jereissati (Coordinator), Javiera F. Medina Macaya, and Stefania Lapolla Cantoni

SURVEY PROJECT COORDINATION: Fabio Senne (Coordinator), Ana Laura Martínez, Daniela Costa, Fabio Storino, Leonardo Melo Lins, Luciana Piazzon Barbosa Lima, Luciana Portilho, Luísa Adib Dino, Luiza Carvalho, and Manuella Maia Ribeiro

STATISTICS AND QUANTITATIVE METHODS COORDINATION: Marcelo Pitta (Coordinator), Camila dos Reis Lima, Isabela Bertolini Coelho, José Márcio Martins Júnior, Mayra Pizzott Rodrigues dos Santos, and Winston Oyadomari

PROCESS AND QUALITY MANAGEMENT COORDINATION: Nádilla Tsuruda (Coordinator), Fabricio Torres, and Patrycia Keico Horie

BRAZILIAN NATIONAL COMPUTER EMERGENCY RESPONSE TEAM – CERT.br
MANAGEMENT: Cristine Hoepers and Klaus Steding-Jessen

CREDITS FOR THE EDITION
EXECUTIVE AND EDITORIAL COORDINATION: Alexandre F. Barbosa (Cetic.br|NIC.br)

TECHNICAL COORDINATION: Tatiana Jereissati and Stefania Lapolla Cantoni (Cetic.br|NIC.br)

EDITING SUPPORT TEAM: Javiera F. Medina Macaya, Leonardo Melo Lins, and Luiza Carvalho (Cetic.br|NIC.br)

Caroline D'Avo, Carolina Carvalho, and Renato Soares (Comunicação NIC.br)

PROOFREADING AND REVISION IN PORTUGUESE: Érica Santos Soares de Freitas

TRANSLATION INTO ENGLISH: Letralia

PROOFREADING AND REVISION IN ENGLISH: Letralia

GRAPHIC DESIGN AND ILLUSTRATION: Pilar Velloso

PUBLISHING: Milena Branco

PHOTOS: iStockphoto

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Digital security [livro eletrônico] : an analysis of risk management in Brazilian companies / Núcleo de Informação e Coordenação do Ponto BR ; [tradução Letralia] ; [editor] Comitê Gestor da Internet no Brasil ; Pilar Velloso. -- São Paulo : Núcleo de Informação e Coordenação do Ponto BR, 2021.
PDF

Título original: Segurança digital : uma análise da gestão de riscos em empresas brasileiras
Bibliografia
ISBN 978-65-86949-38-4

1. Computadores - Medidas de segurança 2. Gestão de risco 3. Internet - Legislação - Brasil 4. Mídia digital 5. Pesquisa - Brasil 6. Proteção de dados 7. Tecnologia da informação I. Núcleo de Informação e Coordenação do Ponto BR.

21-73107 CDD-658.478

Índices para catálogo sistemático:

1. Gestão de riscos : Segurança digital 658.478
Maria Alice Ferreira - Bibliotecária - CRB-8/7964

Brazilian Internet Steering Committee – CGI.br

(IN DECEMBER 2020)

COORDINATOR

Marcio Nobre Migon

COUNSELORS

Beatriz Costa Barbosa
Cláudio Benedito Silva Furtado
Evaldo Ferreira Vilela
Franselmo Araújo Costa
Heitor Freire de Abreu
Henrique Faulhaber Barbosa
José Alexandre Novaes Bicalho
Laura Conde Tresca
Leonardo Euler de Morais
Luis Felipe Salin Monteiro
Marcos Dantas Loureiro
Maximiliano Salvadori Martinhão
Nivaldo Cleto
Percival Henriques de Souza Neto
Rafael De Almeida Evangelista
Rafael Henrique Rodrigues Moreira
Rosauro Leandro Baretta
Tanara Lauschner

EXECUTIVE SECRETARY

Hartmut Richard Glaser

CONTENTS

ACKNOWLEDGEMENTS

The Brazilian Network Information Center (NIC.br), through the Regional Center for Studies on the Development of the Information Society (Cetic.br), would like to thank all the professionals involved in this publication. Our special thanks to Laurent Bernat, from the Organisation for Economic Co-operation and Development (OECD); to Johannes M. Bauer, from the Quello Center of Michigan State University, and to William H. Dutton, from the Oxford Internet Institute of the Oxford Martin School; to researcher Eireann Leverett, from the Centre for Risk Studies of the University of Cambridge; and to Georgina Núñez and Jorge Alejandro Patiño, from the United Nations Economic Commission for Latin America and the Caribbean (UN ECLAC).

We also thank the Brazilian National Computer Emergency Response Team (CERT.br|NIC.br) for their contribution to this publication.

PRESENTATION

Used every day for countless different applications, the Internet has seen tremendous growth in all sectors of Brazilian society in the last ten years, mostly due to its network infrastructure, which is greatly attractive to individuals, organizations, and governments. Specifically in the field of corporate and home applications (the Internet of Things – IoT), the growth of the Internet has also been noteworthy, providing numerous benefits to both individuals and enterprises.

From the social and economic perspective, the fact that more and more people are using the Internet every day, which is very beneficial to society, should be celebrated. However, this expansion has made the use of the Internet increasingly complex, including its association with threats stemming from digital risks and possible security incidents, a tendency that involves devices connected to the Internet and that, to some extent, makes Internet users more vulnerable.

Although technical solutions can mitigate vulnerability risks, which occur naturally in any environment in which a network is open and decentralized, such solutions are not enough to solve these risks. In this context, it is necessary to separate the Internet itself from the applications supported by the network.

Thus, we must be aware of the impacts of different kinds of digital threats so that we can develop a security culture that counters such risks. Although the use of encryption in the applications layer, for example, is a way of using technology to make communication through the Internet safer, it is not enough: many security incidents result from a "social engineering" that explores the vulnerabilities of human behavior.

Therefore, educating Internet users on appropriate standards of conduct is an important component in the search for solutions that minimize the consequences of digital risks. At the same time, it is imperative to preserve and maintain the original principles of openness, collaboration, and cooperation, which have been present since the creation of the Internet, and that have made it such an attractive infrastructure for the extensive range of applications it supports nowadays.

In 2009, the Brazilian Internet Steering Committee (CGI.br) discussed, adopted, and published the Principles for

the Governance and Use of the Internet in Brazil, also aimed at supporting and guiding the committee's actions and decisions. One of the principles specifically recommends that the stability, security, and overall functionalities of the network be actively protected, through the adoption of technical measures that are consistent with international standards and encourage the adoption of best practices. All users that are connected to the network should comply with these recommendations.

Digital security is an instrumental factor for protecting human rights such as privacy and freedom of expression. Moreover, digital security is key for the proper functioning of the Internet and of the entire chain that surrounds it, ranging from its access and services infrastructure to the applications it supports.

In the context of enterprises, this issue has been underscored by the public debate on the digitalization of the economy, especially since the enactment of new laws and the definition of national and sectoral strategies. The Brazilian Digital Transformation Strategy (E-Digital), for example, reinforces the sense of urgency of the digital transformation process, which encompasses the government, the private sector, and society, and which considers confidence in the digital environment as one of its enabling axes.

Another factor which has increased the relevance of the debate on digital security is the crisis unleashed by COVID-19. The pandemic demonstrated even more strongly the importance of digital technologies and, in this context, the Internet became an essential infrastructure for enterprises and their logistic and commercial operations. In addition, the pandemic led to a significant increase in the demand for telework. Hence, as connectivity becomes increasingly critical for enterprises to run their business, digital security for the entire range of devices, software, practices, and standards proves to be a crucial asset, as it is focused on mitigating security incidents and their consequences, which in many cases are difficult to recover from.

In view of this scenario, the present NIC.br Sectoral Studies publication seeks to address issues linked to the management of security incidents and to digital risks. This theme is aligned with the strategies of the Brazilian Network Information Center (NIC.br), aimed at developing the Internet in Brazil, which lead to the production and dissemination of indicators

on information and communication technologies (ICT) that are used to support public policies related to digital security and to expand the debate on this topic.

This publication, jointly developed by the Regional Center for Studies on the Development of the Information Society (Cetic.br) and by the Brazilian National Computer Emergency Response Team (CERT.br), is the result of the cooperation between NIC.br and the Organisation for Economic Co-operation and Development (OECD) in the form of a task force focused on the preparation of an instrument to measure digital risk management practices in enterprises. The five chapters address different themes: economic and social challenges for a secure Internet; the security incident scenario in Brazil; digital risk management for enterprises; a qualitative study on digital risks in Brazilian enterprises; and a proposal for a public policy agenda. Based on these discussions, we hope to contribute with solid indicators on digital security and implications for enterprises.

To conclude, we hope that CGI.br's multistakeholder governance model inspires the engagement of stakeholders in this discussion – so that digital security threats are addressed and that best practices are followed in the management of digital security risks.

Enjoy the reading!

Demi Getschko
Brazilian Network Information Center — NIC.br

PROLOGUE

Laurent Bernat[1]

1 Laurent Bernat is policy analyst at the Organisation for Economic Co-operation and Development (OECD) Secretariat in the Digital Economy Policy Division. He leads the team supporting the Working Party on Security and Privacy in the Digital Economy (SPDE), under the Committee on Digital Economy Policy (CDEP). He led the development of the OECD Recommendations on Digital Security Risk Management for Economic and on Social Prosperity (2015) and on Digital Security of Critical Activities (2019). He currently leads the OECD Global Forum on Digital Security for Prosperity and coordinates policy work on the digital security of products, vulnerability treatment, and "responsible response" by private actors. Prior to joining the OECD in 2003, he worked at the French data protection agency, the Commission Nationale de l'informatique et des Libertés (CNIL) and was associate director in an Internet consulting firm. Laurent Bernat has a master's degree in political science and international relations.

Over the last three decades, concerns with digital security have evolved from technical issues to a key priority for governments and organizations' decision-makers. But what is digital security and what are the main related challenges for government policymakers and other stakeholders? This prologue provides an overarching introduction to policy challenges in this field, from an economic and social perspective. It starts with a discussion on the scope and meaning of digital security, as opposed to cybersecurity. Then, it explains the fundamentals of digital security risk and digital security risk management and introduces some of the main digital security policy challenges for governments.

DIGITAL SECURITY OR CYBERSECURITY?

The first challenge with reference to the theme of digital security is, perhaps, related to terminology in this field. "Cybersecurity" is often used to refer to anything that relates to dangers of using information and communication technologies (ICT): from online bank robbery to possible armed conflicts taking place in the "cyber domain," to espionage, to troll farms destabilizing elections or spreading fake news, to data breaches undermining individuals' privacy.

In fact, there is no officially accepted definition of cybersecurity at the international level because it is often used as a convenient umbrella term for a multifaceted issue covering different dimensions depending on the roles and objectives of the actors concerned. They include *(i)* the technical dimension addressed by ICT experts maintaining hardware, software, networks, and, more generally, information systems; *(ii)* the economic and social dimension, addressed by organizations and individuals aiming at maximizing the likelihood of success of their activities; *(iii)* the criminal law enforcement dimension, addressed by the police and other law enforcement actors tackling online crime; and *(iv)* the national and international security dimension addressed by the military, intelligence agencies and others, such as diplomats involved in conflict prevention.

In practice, experts pursuing these different goals tend to use different terms. For example, ICT security experts gener-

ally talk about "information security," "infosec," or "computer security." Police forces and criminal judges refer to "cybercrime." National security actors talk about "cyberwarfare," "cyberdefense," "cyber operations," "cyberespionage," and even sometimes simply "cyber." In general, the prefix "cyber" tends to be connoted with sovereign functions of the State: police and law enforcement, defense and national security. Therefore, OECD Member countries agreed to use the expression "digital security" rather than "cybersecurity" when referring to stakeholders' efforts to protect their economic and social activities. The term "digital" echoes other expressions familiar to economically oriented civilian non-technical experts, such as "digital economy," "digital transformation," and "digitalization." It is also rooted in the technical reality, as digital security is primarily concerned with issues related to digital technologies, whereas the exact meaning of "cyber" is not immediately clear, even to ICT professionals.

Such terminology distinctions are important because they help acknowledge significant differences in the cultures, tools, jargon and, most importantly, security approaches taken by these categories of actors. While all these actors should work together because their missions are complementary and overlap, they also compete and their methods can come into tension, and even undermine each other.

DIGITAL SECURITY RISKS FOR BUSINESSES

Digital security[2] aims at increasing the likelihood of success of economic and social activities. More precisely, it is the way in which actors address uncertainties affecting the Confidentiality, Integrity and Availability ("CIA triad") of hardware, software, networks and data on which their economic and social activities rely.

Such activities range from simple and mundane to extremely complex and critical; for example, from posting a message on a social network or shopping online, to delivering electricity to millions of businesses and households, or managing hospitals and airports. As the entire economy has become digital-depen-

2 Since it focuses on the economic and social aspects of cybersecurity, this prologue uses the term digital security rather than cybersecurity.

dent to a varying degree, digital security concerns all economic and social activities, including those that are critical to the safety and security of citizens, as well as the functioning of the government and society (OECD, 2020).

Potential events that can harm economic and social activities by breaching the "CIA triad" are caused by intentional or unintentional **threats** taking advantage of **vulnerabilities**. Intentional threats include, for example, attacks from criminals aiming at stealing or extorting money. Unintentional threats include human errors or natural events such as fires, storms, and floods. Vulnerabilities are weaknesses which can be exploited by a threat actor, and include, for example, errors (bugs) in hardware, software, or networks, lack of human training, insufficient protection, whether digital (firewalls) or physical (cameras and locks in a data center), as well as inappropriate procedures (backup processes or disaster recovery plans).

A breach in one dimension of the CIA triad can harm the economic and social activities that depend upon the affected information systems. A **breach of availability** can make a system unusable and stop business activities. So-called Denial of Service (DoS) attacks, which flood a connected system with useless queries, are typical attacks on availability. In 2016, a very large DoS attack affected thousands of servers in parts of North America and Europe, including those of Amazon, CNN, the BBC, and Twitter.[3] A simple power cut can also have a similar effect on an information system.

Breaches of integrity can modify data or the way an information system behaves to disrupt business operations and the delivery of a service, as demonstrated by blackouts that affected over 200,000 people in Ukraine in 2015 and 2016.[4] Ransomware attacks are typical examples of breaches of both integrity and availability. They encrypt data in a system (integrity breach) to make it unusable by legitimate users (availability breach) until money is sent to the attackers who pretend they will decrypt it (but sometimes do not). In October and November 2019, three hospitals in the United States (US),

3 Available at https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

4 Available at https://www.bbc.com/news/technology-38573074 and https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

seven in Australia and one in France faced severe ransomware attacks disrupting their operation to varying degrees.[5] The infamous 2017 WannaCry and NotPetya ransomware incidents, which totalized billions of dollars of damages,[6] hit thousands of businesses and organizations globally. Other attacks have harmed local governments such as in Johannesburg, Baltimore, and the US state of Louisiana.[7]

Lastly, **breaches of confidentiality** enable unauthorized users to access data and potentially violate people's privacy, sometimes at a very large scale. In Brazil, a publicly accessible server exposed the privacy of 120 million citizens because of a misconfiguration issue.[8] In October 2019, the press revealed that a stolen database containing data of 92 million Brazilians was for sale on the dark web.[9] The 2014 data breach at the US Office of Personnel Management showed that governments can also be targeted, with data of over 20 million government officials breached, including sensitive security clearance files and 5.6 million fingerprints.[10] Confidentiality breaches can also affect non-personal data, such as when attackers seek to steal trade secrets. Examples include the German heavy industry giant ThyssenKrupp,[11] European plane manufacturer Airbus,[12] and US energy companies Westinghouse and SolarWorld.[13] Although frequent, attacks against intellectual property are not often reported because affected businesses are reluctant to expose their reputation. According to a 2019 report by the consulting firm PwC for the European Commission, digital

---

5 Available at https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/ and https://www.bloomberg.com/news/articles/2019-11-28/france-not-ruling-out-response-to-cyber-attack-on-hospital

6 Available at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

7 Available at https://arstechnica.com/information-technology/2019/10/johannesburgs-network-shut-down-after-second-attack-in-3-months/, https://arstechnica.com/information-technology/2019/11/louisiana-was-hit-by-ryuk-triggering-another-cyber-emergency/, and https://arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/

8 Available at https://www.zdnet.com/article/over-half-of-brazils-population-exposed-in-security-incident/

9 Available at https://www.cpomagazine.com/cyber-security/citizen-data-of-92-million-brazilians-offered-for-sale-on-underground-forum/

10 Available at https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

11 Available at https://www.cbronline.com/cybersecurity/breaches/thyssenkrupp-cyber-attack-hackers-steal-trade-secrets/

12 Available at https://www.ibtimes.com/hackers-target-airbus-suppliers-quest-commercial-secrets-2833721

13 Available at https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

security-related theft of trade secrets in Europe in 2018 resulted in EUR 60 billion losses to economic growth and almost 289,000 lost jobs; also, projections for 2025 amount to one million job losses.[14] Theft of trade secrets can lead to significant opportunity costs, negative impacts on innovation, increased security costs, and reputational damages. Small and medium enterprises (SME) are easy targets and subject to bankruptcy when theft of innovation or commercial secrets jeopardizes their competitive advantage.

IMPACT OF THEFT OF TRADE SECRETS IN EUROPE

- **Opportunity costs:** including lost business opportunities, lost sales or lower productivity, forfeiture of first-to-market advantage, loss of profitability, or even loss of entire lines of business to competitors. In 2016, 23% of organizations experienced a loss of opportunity due to intrusions, and among them, 42% registered an opportunity loss accounting for more than 20% of its value to the company.
- **Negative impact on innovation:** Research and Development (R&D) does generate a competitive advantage if its results are appropriated by those that invested in R&D. If the results are misplaced and freely used by all, including competitors, then R&D does not bring substantial competitive advantages. Additionally, as long as the threat of cyber-theft continues to grow, companies may become less keen to invest in innovation, due to the risk of misappropriation of their R&D.
- **Increased security costs:** including the annual global expense on cybersecurity software, as well as the cost of cleaning up affected systems and cybersecurity insurance. In this respect, SSP Blue expects that companies across the globe will spend about USD 170 billion on cybersecurity by 2020 (with a growing rate of almost 10% since 2015).
- **Reputational damages:** companies can suffer substantial value depreciation if it becomes public that they have been hacked, including lost value of customer relationships, loss of contracts, and devaluation of trade name. Six hundred mid-sized businesses across six European countries reported the occurrence of reputational damage in 48% of incidents and financial loss in 33% of cases.

SOURCE: PwC (2019).

14 Available at https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

DIGITAL SECURITY RISK MANAGEMENT

Since the early days of computing and until recently, most stakeholders, including policymakers and the OECD, approached digital security primarily as a technical issue: they focused on security risk to systems and networks. However, as losses from digital security incidents increased and became more common, attention shifted from the technical incidents to their economic and social consequences: financial and reputational losses, loss of business opportunities and competitiveness, the impact on privacy and loss of trust, as well as, in some cases, destruction of physical assets and possible loss of lives.

In addition, stakeholders also realized that the security measures aiming at reducing digital security risk can also have negative effects on the economic and social activities they are expected to protect: apart from increasing cost, they can close the digital environment and reduce its dynamism, thus limiting the opportunities to use ICT for innovation. They can also increase time-to-market, reduce performance and user-friendliness. Organizations realized that digital security risk management should primarily focus on economic and social activities rather than on the digital environment that supports them, and that, as a result, it should be led by organizations' business leadership with the support of technical experts rather than the reverse.

Managers in charge of realizing the economic and social benefits of the digital environment are better placed than technical experts to *(i)* set their organization's "risk appetite," i.e., the acceptable level of economic and social risk they can tolerate; *(ii)* assess the possible consequences of digital security risk on economic and social objectives they have the responsibility to achieve; and *(iii)* ensure that security measures do not undermine these activities and reduce the potential of ICT to innovate and contribute to competitiveness.

However, these managers rely on technical experts to understand the possible threats, vulnerabilities, incidents, and options to reduce risk (such as technical security and business continuity measures). Therefore, while both must work together, risk management decisions and responsibility should ultimately be taken by business decision-makers and not delegated to technical experts.

Digital security risk has the following set of characteristics that shape digital security risk management:[15]

- It cannot be entirely eliminated without simultaneously eliminating the opportunities offered by ICT; therefore, some level of digital security risk has to be accepted. Organizations should define and update their digital security risk appetite in order to reduce the risk to the level acceptable to them.
- It is extremely dynamic, therefore digital security risk management never stops. Risk should be assessed and treated on a continuous basis, as part of an ongoing risk management cycle.
- It is not fundamentally different from other types of risks. Therefore, digital security risk management should be integrated into the broader enterprise risk management framework rather than co-exist in parallel as something special.

DIGITAL SECURITY POLICY CHALLENGES

Considering the elements that compose digital security, it is relevant to reflect on the differences among the dimensions of digital security introduced earlier and the challenges they pose to establish appropriate governance framework in governments.

When examining criminal law enforcement, for example, we see that police forces and, more generally, cybercrime frameworks and institutions play an important role in reducing risk at a general level by addressing threats, i.e., deterring criminals from perpetrating crimes and putting them away. While they are not core to an organization's risk management strategy, co-operation with law enforcement is important for legal reasons and to trigger and support investigations after the facts. The police will not generally be best placed to advise organizations on how they should protect themselves from cybercriminals, other than through very general "cyber hygiene" advice, which can hardly take into account the complexity of industrial, business and organizational digital environments.

15 2015 OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. Available at https://oe.cd/dsrm

The subtle balancing exercise to determine which security measures will protect business operations without inhibiting innovation is not a concern for law enforcement.

The culture of institutions and actors in charge of national and international security is also generally different from that of leaders and decision-makers in businesses and other organizations. Risk acceptance is at the core of business culture and security is one among many other parameters in a risk-taking equation, including cost, competition, customer satisfaction, quality, time-to-market, and many others. In contrast, the national security culture is risk averse because its objective is to protect assets with extremely high value for the State, such as national territory or the country's independence. From that perspective, security is above everything because one can assume that everything else will fail if security fails. This may explain why national security culture does not focus on the possible negative consequences of security measures on economic and social activities. For example, solutions such as shutting down systems or banning technologies are often viewed as reasonable means, from a national security standpoint, to eliminate risk, even though they could have very negative consequences on competitiveness if other actors on the global market continue to have access to these systems and technologies. A national security decision over an economic and social challenge can easily undermine prosperity.

It is therefore important to clearly distinguish these areas and not to conflate the different dimensions of digital security into a single concept when developing public policy. At the same time, it is also important to take a holistic and whole-of-government approach encompassing all dimensions to ensure coherence and leverage synergies. Clarifying the governance structure in light of a holistic vision that takes such differences into account is a key objective of national digital security strategies. They generally assign clear responsibilities to relevant agencies, according to their core mission and establish intra-governmental leadership and collaboration mechanisms to facilitate decision-making when interests at stake compete.

A very important aspect of such strategies is to recognize the important role of business, civil society, the technical community, and academia as well as ensure that their voices are

heard, understood, and taken into account, not only when the strategy is developed but also when it is being implemented in the longer term through action plans. Sustainable and trust-based public-private dialogue and partnerships are essential for digital security policymaking, since unbalanced decisions can significantly impact competitiveness, innovation, human rights, freedom of speech, privacy, and other core values of a democratic society. Ultimately, policy effectiveness relies on the ability of large and small businesses, governmental organizations, and individuals to understand and implement policy measures in the long run. Another key challenge for governments is to determine which agency should lead digital security policy, which includes several important areas.

For example, it is necessary to raise awareness and increase the digital security workforce, i.e., ensuring that public and private organizations, businesses, and individuals are aware of digital security risk and understand how to manage them. In addition to communications and public information, this area includes the development of curricula in elementary school but also higher education to train future professionals to fill digital security skills shortages that most countries are facing. Digital security skills are not only technical; they include the capacity for business managers to understand digital security risk and integrate its management in their overarching plans to digitally transform economic and social activities.

Another important area is the development of a digital security industry by encouraging digital security innovation and establishing digital security innovation ecosystems. Several countries have taken a leading role; in particular, Israel with CyberSpark, a joint venture between the national cybersecurity agency, the municipality of Be'er Sheva, the Ben-Gurion University, and the leading companies in the cybersecurity industry, which offers a research center, a R&D hub, a training center, an innovation hub, an incubator, and an intelligence center all in the same location. It is coupled with the CyberSpark Industry Initiative, a non-profit organization (NGO) acting as the central coordinating body for joint digital security industry activities with all stakeholders. Its goals are to leverage the Be'er Sheva region and maximize its potential as a global digital security center, to encourage joint academia

industry partnerships and to attract other national or foreign companies. Other public-private cybersecurity innovation initiative includes the London Office for Rapid Cybersecurity Advancement (LORCA) in the United Kingdom, the Basque Cybersecurity Centre (BCSC) in Spain, and the Innovation Cybersecurity Ecosystem (ICE71) in Singapore. Many of them are part of the Global EPIC, an international network of cybersecurity innovation ecosystems.[16]

The OECD adopted in December 2019 a Recommendation on Digital Security of Critical Activities, which sets out policy recommendations to ensure that policies targeting operators of critical activities focus on such activities to strengthen digital security without inhibiting their capacities to improve services and benefit from digital transformation.

Current important emerging policy trends include fostering policies that encourage the development of more secure products (i.e., goods and services) and to stimulate the adoption of responsible vulnerability disclosure policies by all businesses and organizations.

OECD PROJECT: MEASURING DIGITAL SECURITY RISK MANAGEMENT IN BUSINESSES

The 2015 OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity emphasizes the economic and social dimensions of digital security risk (OECD, 2015).

In 2016, the OECD initiated a project that aimed at increasing the understanding and measuring of the digital security risk management practices of businesses. The first step of this initiative was to review past surveys that had sought to provide data related to digital security risk to understand what kind of data was being produced on the topic. The overall conclusion was that there were few questions on digital security risk management practices of businesses, and when existing, such questions were often limited to technical measures.

Next, the OECD sought to improve measurement in this area by developing a framework to assess the digital security

16 Available at https://globalepic.org/

risk management practices of businesses. This measurement framework, which comprises six modules and 18 associated indicators, guided the design of a survey instrument, developed by Cetic.br|NIC.br, with the goal of understanding the digital security risk management practices, particularly of the specific population of risk managers. The survey instrument was then subjected to cognitive testing in Brazil, also by Cetic.br|NIC.br. The outcomes of this process – the survey instrument together with recommendations – were then reviewed and piloted by the Federation of European of Risk Management Associations (FERMA).[17]

This publication will further explore issues related to digital security risk management, particularly among businesses, as well as the challenges associated with measuring this topic. As part of this effort, it will draw upon the findings of the qualitative work undertook by Cetic.br|NIC.br in Brazil in the process of contributing to the development of the survey instrument for the OECD Project on measuring digital security risk management in businesses.

Laurent Bernat[18]
Organisation for Economic Co-operation
and Development – OECD

17 A report summarising the three phases of the OECD project is available at https://www.oecd-ilibrary.org/science-and-technology/measuring-digital-security-risk-management-practices-in-businesses_7b93c1f1-en

18 The opinions expressed in this document do not necessarily represent the views of the OECD and its members.

REFERENCES

Organisation for Economic Co-operation and Development (OECD). (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion*. Retrieved from https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

Organisation for Economic Co-operation and Development (OECD) (2020). *Recommendation of the Council on Digital Security of Critical Activities*. Retrieved from https://legalinstruments.oecd.org/api/print?ids=659&lang=en

PricewaterhouseCoopers (PwC). (2019). *Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber*. Retrieved from https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

CHAPTER 1

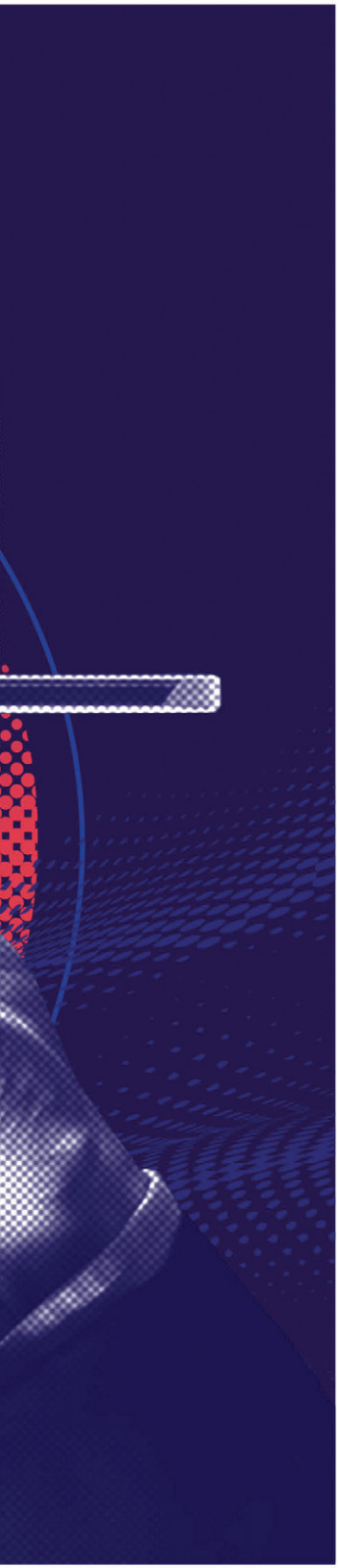
The new cybersecurity agenda: Economic and social challenges to a secure Internet[1]

Johannes M. Bauer[2] and William H. Dutton[3]

1 This chapter is an update and revision of a document originally published on June 2, 2015, prepared to support the World Bank's World Development Report. The authors thank the World Bank and David Satola, in particular, but emphasize that the views and opinions expressed are those of the authors and do not necessarily represent the World Bank or any other organization.

2 Johannes M. Bauer is the Director of the Quello Center for Media and Information Policy and a Professor in the Department of Media and Information at Michigan State University.

3 William H. Dutton is a Senior Fellow at the Oxford Internet Institute, and an Oxford Martin Fellow, supporting the Global Cyber Security Capacity Centre at the University of Oxford. He is also former Director of the Quello Center and a Professor Emeritus at the University of Southern California.



INTRODUCTION

Cybersecurity concerns the "technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor" (Clark, Berson, & Lin, 2014, p. 2). Efforts to bolster cybersecurity are facing a growing range of challenges as the Internet continues to play an increasingly central role in the social and economic development of nations across the world. This is true in every nation, but is particularly the case in the rapidly developing nations, where the Internet's role presents a newer and even more empowering potential for their global role (Dutta, Dutton, & Law, 2011). The range of problems tied to security in the online world is large and growing, and becoming increasingly acute, even though there have been many efforts over the years to enhance cybersecurity. This is, in part, due to the growing centrality of the Internet in economic and social development, making it a more valuable target, but it is also due to the changing dynamics of the problem. Attempts to address these issues have had limited success in many cases, and have not been able to stop the innovativeness of attackers to come up with new strategies, and of users to fall victim to these strategies. Moreover, the same advances in the Internet that, on the one hand, enable more users to bank and shop online more easily, for example, are also making it easier for more individuals to use the Internet for malevolent reasons, such as in virtually democratizing cybercrime.

While concerns over cybersecurity have generated a wide range of initiatives, the problems are persisting and growing in frequency and significance. Arguably, some issues, such as spam, have been well addressed, often due to the potential for technical responses to be diffused widely. Yet even in this case, the problem must be constantly updated: spammers create new ways to reach users, and the incentives behind spamming continue to evolve, such as "spamdexing," aimed at optimizing the visibility of a website in search engines.

Recognition of these growing problems has led many individuals, communities, and institutions to raise the priority of cybersecurity. For example, the launch of the Global Cyber Security Capacity Centre, at the University of Oxford, was met with worldwide interest and generated many commitments to participate in tackling a problem that was widely perceived to exist.[4] While there are cases in which these initiatives have had temporary success in reducing particular problems of cybersecurity, they have not been able as yet to have a lasting impact on a wide range of problems that are perceived to be growing worse as the technology is valued more. Moreover, not all responses have been effective: there needs to be a reconsideration of approaches to cybersecurity that are more sensitive to and aware of the economic and social aspects of the problems, such as why users do not always follow the best practices recommended by the technical security community.

What can be done to support more effective approaches to addressing global and multistakeholder actions to enhance cybersecurity for the digital age? Cybersecurity has been high on the agenda of governments, players in the information technology (IT) industries, and in the many civic groups participating in Internet governance, but paradoxically, the problems are growing and becoming more urgent to address. Because some conventional approaches have not been effective ways of addressing the problem, it is important to challenge conventional wisdom and rethink the ways we address cybersecurity.

NEW FEATURES OF THE EVOLVING CYBERSECURITY LANDSCAPE

The security of telecommunications has been a problem over the centuries, from the use of carrier pigeons to the coming Internet of Things (IoT). Although the Internet was designed to support the sharing of computer resources, including computers and data over networks (rather than to provide security), with the rise of the Internet and its use for more basic activities, such as banking and commerce, the recognition of cybersecurity as a key problem for the Internet

4 More information available at: http://www.oxfordmartin.ox.ac.uk/research/programmes/cybersecurity/

age has increased, albeit not a new issue (NRC, 1991; NRC, 2002; Clark et al., 2014, p. ix).[5]

Technical developments, research, public policy initiatives, and practical steps for users have been evolving over the years to strengthen cybersecurity, such as the global Internet governance community, which has focused its attention on security issues, and this has led to many regional and national initiatives. Examples include organizational innovations as the Internet Corporation for Assigned Names and Numbers (ICANN) forming the Security and Stability Advisory Committee (SSAC) in 2002; the development of the European Union Agency for Cybersecurity (ENISA); the creation of national Computer Emergency Response Teams (CERTs), designed to improve the security of a country; and the creation of Computer Security Incident Response Teams (CSIRTs), which are typically organized with multiple stakeholders (DeNardis, 2014, pp. 90-95). In 2004, the London Action Plan (LAP), an international cybersecurity enforcement network, was founded; focusing on spam, it grew to include 47 government organizations from 27 countries, 28 private-sector organizations from 27 nations, and six observer organizations.[6] There have also been initiatives mainly driven by business, such as the Messaging Anti-Abuse Working Group (MAAWG), formed by members of the messaging industry to address issues such as spam; and there have been global collaborations, such as the global Forum of Incident Response and Security Teams (FIRST.org), which has enrolled more than 300 members from all continents; as well as numerous intergovernmental initiatives such as the Council of Europe's Convention on Cybercrime adopted in 2001, ratified as of April 2015 by 45 countries including six non-European nations.[7]

However, the scale and severity of the problems appear to be rising along with the growing centrality and ubiquity of the Internet in an Internet-enabled, hyper-connected world. In

5 A full range of reports on cybersecurity by the Computer Science and Technology Board of the US National Research Council provides a sense of the history of rising concerns over this issue. More information available at: https://www.nationalacademies.org/cstb/computer-science-and-telecommunications-board

6 Retrieved from http://londonactionplan.org/

7 Retrieved from http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

parallel with the rise of the Internet, there has been a commensurate growth in cybercrime: problems with spam continue to be a problem for Internet Service Providers (ISPs) and users (Krebs, 2014), and threats to privacy have been growing with the development of social media and Big Data computational analytics, threats that were dramatically exposed by the revelations of Edward Snowden in 2014.[8]

Nevertheless, efforts to address the problems have not been sufficient to reduce what appears to be a rising array of cybersecurity problems. There are many reasons for the difficulties confronting cybersecurity initiatives. Many key actors, including users, have been slow to adopt practices that could enhance their security online. Therefore, motivating a wide range of actors across the globe, exceeding four billion users, to change the way they do things is not only a technical issue. It also requires an understanding of how each actor views cybersecurity, such as their level of awareness, and how they are incentivized to ignore or adopt practices that could protect themselves and others in the online environment. In general, the provision of cybersecurity is often difficult and costly, which might mean that accepting some level of insecurity is economically rational (Anderson & Moore, 2006; Moore, Clayton, & Anderson, 2009), such as when individuals accept the potential risks of online commerce, or when organizations decide to accept the costs of compensating victims rather than impose security precautions that may be perceived as cumbersome or off-putting by customers.

Several developments on the cybercrime side also contribute to the potentially wicked nature of the problem.[9] For example, the virtue of global connectivity enables criminals to launch attacks remotely, using servers and machines in other countries. Anonymity raises another limitation on cybersecurity initiatives, which is the need to balance security with other valued objectives, such as privacy and freedom of expression. One real risk of the push for cybersecurity is the potential to undermine other key values and interests that can be enhanced

8 Retrieved from http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

9 The concept of "wicked problem" is meant to emphasize problems that are exceedingly complex, dynamic, and difficult, if not impossible, to solve.

over the Internet. Therefore, there is a need to balance these sometimes compatible but sometimes competing objectives, such as the "tensions between cybersecurity and surveillance" related to national security (Clark et al., 2014, pp. 104-105).

One consequence of these developments has been an increasingly central focus on the role of social and behavioral issues in addressing cybersecurity. Too often, cybersecurity has been left to the computer experts in the computer sciences and engineering, or to the information technology team in an organization. While their technical knowhow and contribution to a secure organization, as well as to a secure, open and global Internet has been and will remain great, initiatives to address growing problems with cybersecurity face several new challenges that require contributions from many more disciplines and actors.

CHALLENGES FOR ADDRESSING CYBERSECURITY

1. A new range of actors and motivations

The Internet and information and communication technologies (ICT), such as social media, mobile Internet and IoT, are expanding the range of actors involved in protecting security, especially users, who are seldom focused on security, except as a necessary step to moving ahead with what they wish to do online. At the same time, the range of actors who are capable and willing to attack information systems is also broadening, spanning a wide range of motives from attacks on national security to other criminal motives.

2. An expanding range of platforms and applications

Gone are the days of protecting security on an organization's mainframe computer; now, an expanding array of platforms – from social media to the World Wide Web, as well as mobile platforms, cloud computing, Big Data and the IoT – are creating a far more complex set of technological platforms and social settings that have somewhat different characteristics and require somewhat different approaches to security. Some are dependent on the weakest link in a system of connected nodes, such as the use of botnets, while others are dependent on the efforts of specific actors, such as in the case of targeted attacks on a company or a State (Varian, 2004).

The increasing availability of broadband Internet access since the late 1990s has greatly boosted Internet use, but also multiplied vulnerabilities. Moreover, the rapid adoption of mobile phones and devices, as well as the networking of an increasing number of objects in IoT, has further increased the number of attack points and expanded the footprint of cybercrime to developing countries (Orji, 2012; Shalhoub & Al Qasimi, 2010).

With the massive use of mobile devices and social media, new strategies are on the rise. The mobile application marketplace is also increasingly used, often using fake versions of popular applications. While mobile devices typically detail the permissions sought by an application, mobile users too often accept an app without critical examination. Access to other functions such as bluetooth, GPS, and a camera, in addition to personal data, offers a broader attack surface than traditional computers.

3. Balancing a wider range of issues

Security can no longer be viewed discretely, as it is closely connected with other issues, such as privacy and surveillance, as noted above, and with the risks associated with the new media generally, such as threats and harms tied to the use of social media. Given this interdependence, it is necessary to identify and consider trade-offs that may exist with other goals, such as when increasing security might compromise freedom of expression or personal privacy. This is a difficult task, since users might well sacrifice some values, such as privacy, for security, or even convenience (Dutton & Meadow, 1987). It is therefore important for governments and other stakeholders to ensure that rights and responsibilities are protected in the course of ensuring greater cybersecurity.

4. Interdependent multi-level governance issues

Governance issues are entangling enterprises, government agencies, nations, regions, and global actors in an increasingly interdependent range of governance processes. Recognition of the global scale and interdependence of these issues is critical to avoiding the risks of a fragmentation of governance that could undermine local and global initiatives, not only around cybersecurity, but also around all the issues tied to the Internet

– from the privacy of individuals to the vitality of global commerce. The Internet does not have clear national boundaries, making the success of cybersecurity an increasingly worldwide challenge that cannot be contained within any single organizational or national boundary.

5. Awareness of practices as well as problems

Public and organizational awareness campaigns have been undertaken for decades, but most often, these are based on frightening users. Much more effort needs to be focused on giving users tips and guides to best practice on how to protect their own security and help protect the safety and security of other users. To be successful, these campaigns need systems to be designed in ways that are easy for individuals to use.

6. Improving user-interface designs for security applications

Many of the security systems designed by the technical community are becoming increasingly infeasible for users to apply. New designs need to be developed and implemented more widely to make it easier for users to protect themselves and their computers from security breaches, without compromising other important values and interests of theirs, such as protecting their anonymity, convenience, or speed in obtaining a service.

7. The dual effects of technological advances

A last and overarching issue that is not new but increasingly apparent, is the dual effects of empowerment. Cyberthreats are evolving rapidly in a technical race, pitching efforts to increase security against attempts to find new ways to breach it by malevolent actors. These hostile actors range widely as well, including malevolent hackers[10] and ordinary criminals, who increasingly find cybercrime easy and safer than the physical commission of a crime, such as a burglary.

---

10 A "hacker" was initially defined as a person who was obsessively focused on solving a programming problem, what Joseph Weizenbaum (1976, pp. 111-131) referred to as a "compulsive programmer." The author's concern was that such a compulsion would undermine humanistic knowledge of a problem and create technicians rather than programmers. Since Weizenbaum (1976), the term has been used more often to define individuals who seek to break into, "hack," or crack computer systems, increasingly through the Internet.

THE DISTRIBUTED COSTS AND BENEFITS OF CYBERSECURITY

To understand the dynamics of cybersecurity, it is critical to know who gains and who pays for greater or lesser levels of security. However, the actual costs and benefits of cybersecurity continue to elude efforts to develop reliable and valid quantitative indicators. Although estimates of the costs of cybercrime abound, many reports are based on weak evidence and/or overly simplified, strong assumptions. Often, the employed methods are not publicly available, complicating an assessment of the validity and reliability of the information. Hence, damage is typically assessed at a highly aggregated level and difficult to link to specific incidents.

Recent developments of more robust methods of measurement focus on individual enterprises and organizations and not on the entire value network or costs to society at large, which would be the relevant metrics for public policy and law-enforcement decisions. The numbers reported are sometimes puzzling, and detailed explanations for their variations are absent.

Because of the highly interconnected nature of the Internet, security incidents not only affect the immediate targets of an attack, but they also have second- and third-round effects on other stakeholders. From a public policy perspective, the relevant cost is the total cost to society, which also includes the costs incurred by stakeholders other than those immediately affected.

A comprehensive assessment of the costs and benefits of cybersecurity should therefore include the entire ecosystem of players, including:

- users (individuals, households, and large, small and micro businesses);
- private-sector organizations involved in e-commerce (online merchants, financial services, insurance services, health, etc.);
- public-sector organizations (e-government services);
- IT infrastructure providers (software vendors, ISPs, hosting providers, registrars);
- incident response units (CIRTs, law enforcement);
- society at large (including opportunity costs, lost efficiency gains, diminished trust and use of the Internet, etc.); and

- criminals and malevolent actors (including cybercriminals, malevolent hackers, and all those seeking to profit from undermining the security of the Internet).

When assessing the impact of a particular security incident, for example, it is helpful to distinguish between these direct and indirect costs (Gordon & Loeb, 2005). Direct damages are costs that are caused by a specific security breach. Indirect costs, while certainly caused by the fact that a security breach occurred, are not simply the consequence of a specific breach, rather, they reflect more generic costs, such as the cost of measures to prevent security breaches or the cost of training personnel to adopt security practices.

Direct and indirect costs can be either explicit or implicit (Gordon & Loeb, 2005). Explicit costs, such as security expenditures, are well defined and, in principle, directly visible from cost-accounting data. Implicit costs are known impacts of security breaches that often elude unambiguous measurement, although it may be possible to find proxies. Implicit costs at the level of society at large occur, for example, if security problems slow down the adoption of online services by market players and end users, thus retarding society-wide benefits extending from use of the Internet.

Based on this categorization, different specific costs can be identified. Using this framework, systematic assessments of the total cost of cybersecurity can be put together in a step-by-step process. Individual steps are repeated until all cost categories have been scrutinized as to whether they are relevant for each of the actors and, if they are, the magnitude of the direct, indirect, or implicit impact can be estimated. Adding each type of cost across all players and cost categories yields an estimate of the total direct, the total indirect, and the total implicit costs.

Recent research has found an interesting relationship between increasing connectivity and threats to information security. As connectivity in a country increases, problems with cybersecurity initially increase. However, this is not linear: as adoption rates further increase, this trend is reversed, and security performance increases again (Burt, Nicholas, Sullivan, & Scoles, 2014). This observation highlights the challenges faced by developing countries: at the same time, as capacity

building and education, as well as enlightened policies, are important factors in reversing the trend, these findings also offer encouragement and a way forward, as things might get worse before they get better.

(DIS)INCENTIVE STRUCTURES ACROSS THE MULTIPLE STAKEHOLDERS

The distributed costs and benefits of cybersecurity can create major incentives for some users to engage in malevolent activities, such as phishing: a malevolent website might try many (20 or more) times to get access to a particular computer, such as through phishing. In contrast, the incentives are relatively low for many users, leading them to lack caution now and then in seeing a suspicious e-mail or message.

UNDERSTANDING THE DIVERSITY OF INCENTIVES

The multiplicity of motives across users needs to be considered in understanding their behavior. For example, the motivations of hackers vary widely, from "white hat" hackers (mainly motivated by beneficial goals) to "black hat" hackers (mainly motivated by malevolent motives). Just as the Internet has tended to democratize access to information, it has also tended to democratize some criminal activities by making it easier for non-computer experts to use the Internet to commit crimes, such as fraud, leading some to talk about the "democratization of cybercrime."

For example, "white hat" hackers may be engaged in attacking systems with the aim of making them safer, or to hold organizations more accountable, such as by exposing fraud. Governments may have an interest in keeping vulnerabilities to be able to penetrate systems operated by adversaries, an example of how cybersecurity can be in tension with national security, as shown by the continuing controversies over encryption. In this interaction, efforts to secure systems and devices and educate users to adopt safe online behaviors are regularly undermined with new and innovative technical and social means. Reducing the threats from one generation of attack vectors may be a temporary success until new forms emerge, while the threat landscape also varies in response to the deployed communication platforms and devices, and the

services used by businesses and individuals, as well as the economic, legal and institutional framework of a place.

Threats have changed from a time of highly visible attacks by intruders in search of fame, glory, and notoriety, to largely invisible attacks driven by fraudulent and criminal motives. For a time, viruses were a main concern and e-mail spam was a major vehicle for the dissemination of malicious code; as hardware manufacturers, software developers, ISPs, and users have adapted to these challenges, attack strategies have also changed.

THE POLITICAL ECONOMY OF CYBERSECURITY[11]

One of the major reasons why efforts by multiple stakeholders to address problems of cybersecurity have not had a more sustained impact has to do with the particular "problem structure" of information security challenges (Asghari, Van Eeten, & Bauer, 2016). The Internet is a dense network with numerous technological and economical interdependencies between key players; also, information security has strong public-good characteristics in that its benefits accrue to the community of users at large. Both costs and benefits often affect multiple players without market transactions to compensate for them; in other words, information security is typically afflicted with positive and negative externalities.

Furthermore, markets for security as well as markets for many media and information services suffer from problems of incomplete and asymmetrically distributed information. Users are generally not in a position to evaluate the security performance of an ISP, a device, software, or an application; so, the exact nature of how externalities and information asymmetries affect security varies depending on the type of security risk, the nature of attacks, and the best defenses.

For instance, take the case of untargeted attacks. If a user forgoes investment in security software for an Internet-connected device and this machine becomes infected, this may affect its performance, but the main cost of security incidents will be borne by others to whom the machine sends malware. Hence, an unprotected or under-protected user causes a negative exter-

11 This section relies heavily on the research reported in Van Eeten, Bauer, Asghari, & Tabatabaie (2010) and Van Eeten & Bauer (2013).

nality for others. If, on the other hand, a user invests in cybersecurity, some of the benefits will accrue to other users, whose machines will be less likely to be infected.

In this sense, the user causes a positive externality. Therefore, given that only part of the costs associated with a negative externality are borne by the user causing it, and only part of the benefits of a positive externality are enjoyed by the user causing it, decentralized decision-making by individual users will systematically not reflect these broader spillover effects on the larger ecosystem. However, the opposite is true for targeted attacks: an organization fortifying its defenses against targeted attacks inadvertently exerts a negative externality on other organizations that did not undertake similar security measures, and consequently face a higher risk of an attack.

An increasing volume of research argues that many cybersecurity problems are caused by misaligned incentive structures, which (dis)incentivize individual actors and therefore, given these interdependencies, result in greater security problems for all. Literally, all participants in the Internet ecosystem work under mixed incentives, some contributing to enhanced security efforts, other weakening them. The net effect of these conflicting forces is often ambiguous, but they need to be the focus of study.

A brief explanation is presented below to illustrate key incentives for important players in the Internet ecosystem.

THE INTERNET ECOSYSTEM: KEY PLAYERS AND INCENTIVES

HARDWARE VENDORS

Hardware manufacturers operate in a highly competitive marketplace. Testing hardware and its components for possible vulnerabilities may increase time to market and, in the presence of first-mover advantages and network effects, delay could result in lasting disadvantages. At the same time, equipment manufacturers need to be concerned about their reputation. The first factor reduces attention to security and the second increases it, at least if reputation is also dependent on security performance: if reputation effects are stronger, the net effect will be

increased security. Another vulnerability introduced into the Internet ecosystem is the practice of bundling hardware with trial versions of security software and others. These conflicting incentives could be addressed by increasing secure equipment design practices, establishing minimal standards for equipment, adopting manufacturer liability rules, and changing the default to automatic software renewal and updates.

SOFTWARE VENDORS

Like hardware vendors, software vendors work under ambiguous incentive structures. The cost and time (time to market) of software testing constitutes a potentially security-reducing factor. The user's desire for high levels of functionality, compatibility, and discretion often comes at the cost of security features. Software licensing agreements that contain hold-harmless clauses shield the vendor from any legal action and, hence, all other things being equal, weaken the incentive for software vendors to invest in security. Moreover, software is developed in a diverse range of institutional forms, from commercial enterprises to peer production, to individual amateur programmers; therefore, not all applications, plugins and programs are developed with security in mind.

INTERNET SERVICE PROVIDERS (ISPs)

ISPs are key players in the Internet ecosystem, with numerous options to enhance information security. The costs of customer support and abuse management, as well as the cost of additional infrastructure that might be required to handle malicious traffic, all have an immediate effect on the bottom line and have increased incentives for ISPs to undertake security-enhancing measures. Loss of reputation and brand damage work indirectly (and probably more slowly) but exert pressure in the same direction. ISPs are embedded in an interdependent system of service providers that can activate a range of escalating options to retaliate against poor security practices, such as blacklisting, even if the origin is an individual user. In contrast, the costs of increasing security, legal provisions that shield ISPs from legal liability, and the costs of customer acquisition constitute factors that tend to reduce investment in information security.

USERS

Large businesses (enterprises with 250 or more employees) that use the Internet are a heterogeneous group; many have adopted risk assessment tools to make security decisions, but the diligence they exercise will vary with their size (their scale enables them to have a greater capacity of cybersecurity) and other factors, such as the specific products and services provided. Small and medium enterprises (SME, typically defined as enterprises with less than 250 employees), micro-enterprises, and residential users are a large and diverse group. Like other participants, they work under multiple and potentially conflicting incentives. Many SME, micro-enterprises, and residential users have insufficient resources to create cybersecurity capacity to prevent or respond to sophisticated types of attacks. Large businesses and individual users may suffer from the perception that their own risk exposure is low, whereas many SME and residential users will invest in security – and some may even over-invest –; this way, there is no guarantee that the effort level will be optimal. For example, many nations have high levels of pirated software that cannot be automatically updated, which is an inherent security risk.

GOVERNMENT

Government and government agencies, in principle, are actors who could align these incentives of different actors by developing effective policies. For example, "Cyber Essentials,"[12] a policy adopted in the United Kingdom that incentivizes contractors who wish to work on government contracts to implement certain minimal security practices, suggests that such policies for contracting can contribute to security improvements. Yet, governments are not always the neutral and beneficial actor they could be: government agencies are the largest purchasers of "zero-day exploits" – vulnerabilities of software, for example, which are not yet known to the vendor –, as it enables them to gain access to the strategic assets of rival forces. Hence, conflicts of interest may exist within secret service organizations,

12 Retrieved from https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

the military and other government organizations that result in uneasy tensions and ambiguous overall incentives.

THE NEW AGENDA FOR THE NEW CYBERSECURITY LANDSCAPE

The theme running through this chapter, in reviewing the social and economic aspects of cybersecurity, is the need for a wider array of actors to reconsider approaches to achieving greater cybersecurity. Conventional approaches, evolving from the era of mainframe and then personal computers, were dominated by the computer-security technical community and relatively centralized in the computer-support teams of governments, business and industry, and service providers, such as banks. The twenty-first century Internet has put users increasingly at the center of approaches to cybersecurity, while the role of the computer expert is being limited by their understanding of users.

Internet users are diverse and might have overly simplistic or even erroneous mental models about secure and insecure behaviors online (Dutton, 2017), but these must be understood by the security community, such as network operators, who are another key actor in increasing security (Wash & Rader, 2011). Likewise, app designers and software developers play a critical role but often do not follow secure design practices, or understand the knowledge and practices of their users. In addition, developing approaches are being organized in the Internet age of decentralized, user-centric computing, where the role of computer experts is increasingly limited and the role of the user and a wide array of other actors is greatly expanded in the new Internet ecosystem.

In light of such developments, there are new ways to address the rising challenges facing cybersecurity by focusing more on the economic and social dimensions of the problems, which include:

- understanding the role of a multiplicity of users in the new Internet landscape;
- knowing more about the real and perceived costs and benefits shaping the behavior of these actors;
- mapping the incentive structure underpinning responses to cybersecurity in ways that can guide policy initiatives designed to restructure incentives; and

- describing the attitudes, beliefs, and practices of users to enable software and systems for cybersecurity to be designed in order to be in sync with user expectations and behavior.

MOVING FORWARD: THE NEW CYBERSECURITY AGENDA

CYBERSECURITY CAPACITY BUILDING

At every level – nation, organization, and individual – there is a need to build a capacity to maintain security online. Currently, the elements of cybersecurity capacity building are being identified through several projects and collaborative efforts, such as the Oxford Cybersecurity Capacity Building Model. This group advocates an approach at multiple levels, including: using technologies to control risks; building cyber skills, from the workforce to leadership; creating effective legal and regulatory frameworks, including cyber policies and defenses; and encouraging a responsible cyber culture within society.[13]

There is a growing recognition of a lack of cybersecurity expertise. Many computer science departments in North America and Western Europe have had a cybersecurity or computer security program in place for years, and an increasing number of courses are focused on this issue. However, there remains a skills gap in most nations, and a clear need to grow the numbers of cybersecurity experts worldwide and to expand curricula to include a greater focus on users and the social and economic aspects of cybersecurity.

Similarly, the size of corporate and other organizational budgets directed to cybersecurity is generally insufficient. Not only is this function viewed too often as a low priority, but it can sometimes be seen as a threat to the core business of the organization, and viewed as the "business prevention unit."[14] There is a clear need to change the image of cybersecurity as it increasingly becomes a key aspect of a corporation or organization's reputation.

---

13 More information available at: https://www.oxfordmartin.ox.ac.uk/cyber-security/

14 A point made by a cybersecurity expert at a conference, but for which we cannot attribute the quote.

MORE REALISTIC USER-CENTERED DESIGNS FOR SECURITY

Instead of blaming users for not adhering to impossible guidelines on the protection of systems, such as the memorization of multiple passwords, systems need to be designed in ways that users can manage better. Users, from students to retired persons, are seldom interested in cybersecurity *per se*: they want to get their job done online, whether that is listening to music, filing taxes, or contacting their family. If they have to deal with security, then they want something convenient, simple, easy to use, and that works everywhere. This goal might well be impossible to meet in its entirety, but that is the direction that designs should move towards.

Most generally, more work needs to address human-computer interaction that is focused on the security area and that entails behavioral research on what users actually do.

LEARNING AND EDUCATION: MOVING FROM FOSTERING FEAR TO EDUCATING USERS

Although cybersecurity initiatives have often had a public awareness component, these are most often focused on frightening individuals into being more protective of their security online. In general, fear campaigns do not generally work, in part because they do not give clear and practical instructions on what to do. This is difficult because there are only a few conventional strategies for users to follow. Moreover, they might well have negative consequences, such as undermining trust in using the Internet for social and commercial activities, which could hinder the use of the Internet generally, or differentially, lead to increasing digital divides as users at the margins, such as the elderly, might be frightened, while more experienced users remain confident.

In addition, it is important to find ways to move beyond "campaigns" to make cybersecurity an essential part of more basic and lifelong learning and education. We teach people how to write, draft a letter, speak to a group, but we seldom train children and others to use e-mail, social media, and related technologies in a safe, ethical, and appropriate way. Learning how to use the Internet in appropriate ways, that reduce potential harm to others and respect the dignity of other users, needs to be a central part of educational pro-

grams across the life span. Some risks related to social media, such as cyberbullying and sexting, require users to identify and understand potential risks and how to minimize them. All aspects of cybersecurity should be incorporated in this lifelong learning about the appropriate and safe use of the Internet and related ICT.

Ideally, learning and education, reinforced by social norms and pressures, could lead to the development of a "cybersecurity mindset" (Dutton, 2017). Internet users might well develop a mindset that makes security an aspect of what they do without thinking about it each and every time. This is a cultural change, but it is possible and will be made easier if security is better designed for users.

In addition to individual users, education and learning are increasingly important for small, medium and micro-enterprises. A very large proportion of businesses fall into this category, and their use of the Internet and online commerce are critical for their economic development. Thus, providing them with a genuinely stronger sense of security and a better understanding of how to protect themselves in the cybersecurity area could be a critical role of national and international organizations.

RESTRUCTURING INCENTIVES

Some actors in the cybersecurity ecosystem have strong incentives. Spammers have real financial incentives (Krebs, 2014); an analogy is the telemarketer, who might get a positive response from a very small percentage of those targeted by a marketing message, but given the low cost of reaching this market and the value of sales, the effort is, nevertheless, highly profitable. Likewise, many spammers continue because of the economic incentives behind their activities. Of course, the IT team in charge of protecting computer security is also incentivized, as their jobs might be on the line.

However, many actors in the ecology of the Internet do not have strong incentives to prioritize cybersecurity or they demand that others in the value network provide security (for example, network operators argue that users are responsible, while users argue the opposite). Too often, the costs of the lack of security are externalized, as individuals perceive others to

benefit and others paying the costs, such as their bank, or credit card company, or society at large.

Also, experience often beats rational concerns. Our own research has found that the Internet is an "experience technology," that is, users trust the Internet more as they gain experience with it. Nevertheless, bad experiences online can reduce that trust (Blank & Dutton, 2011), and there is evidence of growing concerns over privacy and surveillance that could erode trust in the Internet (Dutton, Law, Bolsover, & Dutta, 2014).

New mechanisms, such as cybersecurity insurance, need to be devised to restructure these incentives, in order to lead more actors to see a stake in protecting their own cybersecurity. Insurance, for example, would make users more accountable for their security, such as if their premiums were dependent on their ability to protect themselves, thus creating an incentive for good behavior. There might be other incentives, beyond saving or losing money, such as the loss of a service tied to insecure practices, such as being forced to update a password in order to restore an e-mail service. All of these strategies have potential risks, such as undermining the marginal users and deepening the digital divide, which is why it is critical to explore ways to restructure the incentives underpinning cybersecurity.

MAKING CYBERSECURITY AN ASPECT OF LOCAL AND GLOBAL INTERNET GOVERNANCE

Cybersecurity cannot be achieved unless policy and practice can be increasingly global: this is both a cultural and a governance challenge in that nations do not place the same priority on key values and interests and practices, such as the importance of anonymity. Therefore, there need to be venues for resolving these cultural differences and coordinating international responses.

While some moves toward "data localization" could be restrictive and undermine the benefits of a global Internet (Bauer, Lee-Makiyama, van der Marel, & Verschelde, 2014), others could enable more flexibility locally and internationally. For example, the Internet does not require all nations to move to some lowest common denominator; banks sometimes need to ensure their government and customers that they are subject to a particular regulatory regime, and therefore, con-

tract their cloud services in ways to keep their data within their national boundaries. Governments might also localize some services that enable features that other jurisdictions might not allow, such as the right to anonymity for political speech. Rather than treat all data and information in the same ways, the Internet has tremendous malleability that would enable creative solutions to address local and international issues of privacy, freedom of expression, and cybersecurity.

BALANCING CYBERSECURITY WITH THE BROADER ECOLOGY OF INTERNET POLICY CHOICES

It is impossible to deal with cybersecurity as a single issue when in fact it is tied to many related issues in a broad ecology of policy choices, such as around privacy, surveillance, and freedom of expression. Most stakeholders want to promote not only a secure Internet, but a global, open, and secure Internet; therefore, a myopic focus on cybersecurity could undermine other values and interests.

The mission and expertise of cybersecurity experts must be increasingly balanced by the goals and expertise of those with other roles and other types of expertise in law, public policy, and use of the Internet and related media. Some major online commercial enterprises, for example, have been able to provide easy access for online shopping and secure payments, in relatively easy-to-use and reliable ways.

Lastly, the case must be more clearly made that cybersecurity is becoming a requirement or necessary condition to protect privacy, for example, as well as the financial vitality and reputation of a business. Cybersecurity needs to be perceived as an enabler of other goals, rather than in conflict with their achievement; but this requires system designs to address the skills, attitudes, and behavior of their users.

CONCLUSION

The Internet and related ICT are becoming increasingly central to the economic prosperity of developing and developed nations. However, the benefits of the Internet and related technologies are contingent on maintaining a level of security, trust and openness of a global Internet. While the Internet can empower individuals, organizations, and nations of the

developing world in an increasingly global economy, the same technology also appears equally able to empower hostile and malevolent actors, who have strong economic and social incentives to pursue their attacks. Clearly, success depends on global efforts to address the challenges to cybersecurity, and a central global question arises: how can the world reap the huge economic and social benefits of the Internet and, at the same time, ensure its security?

There is no solution to cybersecurity – no *Deus Ex Machina* on the horizon. It is a constantly moving target that will entail a continually evolving set of processes to contain the security risks associated with the use of the Internet and related digital media. Moving forward on the development of these processes will inevitably be a matter of incrementally adapting and improving existing approaches; in organizations this is often called "muddling through," rather than seeking to find a rational-comprehensive solution.

There are too many actors and security problems across the globe and platforms for there to be a neat, one-size-fits-all global solution to cybersecurity. Given the dynamic nature and complexity of progressing in this area, there is a need to accept a long-term process of incremental decisions that enable actors to muddle through to find better solutions over time. In this sense, this paper has pointed to directions for moving current approaches to cybersecurity, such as revitalizing public-awareness campaigns by focusing on providing tips for addressing problems rather than generating fear on the part of users. These approaches suggest a new agenda for a changing cybersecurity landscape.

While the economic and social potential of the Internet is great for all nations – developing and developed alike –, these benefits are increasingly at risk of failing in light of risks tied to the lack of security and falling levels of trust in the Internet and those who manage and exploit this technology around the world. Many authors question if we are in an Internet "trust bubble" (Dutton et al., 2014); however, there are clear ways in which cybersecurity can be better approached once we recognize the new aspects of cybersecurity in the digitally connected world and the centrality of users in this new ecology of choices shaping the future of the Internet.

REFERENCES

Anderson, R., & Moore, T. (2006, October 27). The Economics of Information Security. *Science,* 314(5799), 610–613. doi 10.1126/science.1130992.

Asghari, H., Van Eeten, M. J. G., & Bauer, J. M. (2016). The Economics of Cybersecurity. In Bauer, J. M., & Latzer, M. (Eds.). *Handbook on the Economics of the Internet* (pp. 262-287). Cheltenham, UK; Northampton, MA: Edward Elgar.

Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). *The Costs of Data Localisation: Friendly Fire on Economic Recovery*. ECIPE Occasional Paper, n. 3. Bruxelas, BE: ECIPE. Retrieved from https://ecipe.org/publications/dataloc/

Blank, G., & Dutton, W. H. (2011). Age and Trust in the Internet: The Centrality of Experience and Attitudes Toward Technology in Britain. *Social Science Computer Review, 30*(2), 135-151.

Burt, D., Nicholas, P., Sullivan, K., & Scoles, T. (2014). *The Cybersecurity Paradox: Impact of Social, Economic, and Technological Factors on Rates of Malware*. Microsoft Security Intelligence Report. Retrieved from http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity-Risk-Paradox.pdf

Clark, D., Berson, T., & Lin, H. S. (Eds.). (2014). *At the Nexus of Cybersecurity and Public Policy*. Computer Science and Telecommunications Board, National Research Council. Washington DC, VA: The National Academies Press.

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven, CT; London, UK: Yale University Press.

Dutta, S., Dutton, W. H., & Law, G. (2011, April). *The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online: The Global Information Technology Report 2010-2011*. New York City, NY: World Economic Forum. Retrieved from http:// ssrn.com/abstract=1810005

Dutton, W. (2017). Fostering a Cyber Security Mindset. *Internet Policy Review, 6*(1). DOI: 10.14763/2017.1.443. Retrieved from https://policyreview.info/node/443/pdf

Dutton, W. H., & Meadow, R. G. (1987). A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties. In Levitan, K. B. (Ed.). *Government Infostructures* (pp. 147-170). Westport, CT: Greenwood Press.

Dutton, W. H., Law, G., Bolsover, G., & Dutta, S. (2014). *The Internet Trust Bubble: Global Values, Beliefs and Practices*. New York City, NY: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf

Gordon, L. A., & Loeb, M. P. (2005). *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. Columbus, OH: McGraw-Hill.

Krebs, B. (2014). *SPAM Nation*. Naperville, IL: Sourcebooks, Inc.

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. *Journal of Economic Perspectives, 23*(3), 3-20.

National Research Council (NRC). (1991). *Computers at Risk: Safe Computing in the Information Age*. System Security Study Committee, Commission on Physical Sciences, Mathematics, and Applications. Washington DC: The National Academies Press. Retrieved from https://www.nap.edu/catalog/1581/computers-at-risk-safe-computing-in-the-information--age

National Research Council (NRC). (2002). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Computer Science and Telecommunications Board, Division of Engineering and Physical Sciences. Washington, DC: National Academy Press. Retrieved from https://citadel-information.com/wp-content/uploads/2012/08/cybersecurity-today-and-tomorrow-pay--now-or-pay-later-national-research-council-2002.pdf

Orji, U. J. (2012). *Cybersecurity Law and Regulation*. Nijmegen, NL: Wolf Legal Publishers.

Shalhoub, Z. K., & Al Qasimi, S. L. (2010). *Cyber Law and Cyber Security in Developing and Emerging Economies*. Cheltenham, UK; Northampton, MA: Edward Elgar.

Van Eeten, M. J. G., & Bauer, J. M. (2013). Enhancing Incentives for Internet Security. In Brown, I. (Ed.). *Handbook of Internet Governance* (pp. 445-484). Cheltenham, UK: Edward Elgar.

Van Eeten, M. J. G., Bauer, J. M., Asghari, H., & Tabatabaie, S. (2010). *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data*. STI Working Paper 2010/5. Paris, FR: OECD.

Varian, H. (2004). System Reliability and Free-Riding. In Camp, L. J., & Lewis, S. (Eds.). *Economics of Information Security* (pp. 1-15). Berlin, DE; New York City, NY: Springer.

Wash, R., & Rader, E. (2011, September). Influencing Mental Models of Security. *Proceedings of the New Security Paradigms Workshop (NSPW), 11,* 57-66. Retrieved from https://dl.acm.org/doi/10.1145/2073276.2073283

Weizenbaum, J. (1976). *Computer Power and Human Reason: From Judgment to Calculation*. San Francisco, CA: W. H. Freeman and Company.

CHAPTER 2

Cyber risk management for small and medium enterprises

Éireann Leverett[1]

To measure is to know.
JAMES CLERK MAXWELL, 1831-1879

1 Éireann Leverett is founder of Concinnity Risks, a boutique cyber risk consultancy. He is also a senior risk researcher at the Centre for Risk Studies at the University of Cambridge and coauthor of Solving Cyber Risk. Éireann enjoys quantifying cyber risks, collaborating with incident response teams, taking long walks in the forest, and learning about foraging and natural navigation.

To play better, we must keep score; to keep score, we must measure. Although this may seem obvious, how do we approach measuring cyber risk management for small and medium enterprises (SME)? Much of what goes on with computers and data is invisible and it is only possible to manage risks correctly when we find an easy way to measure them.

This article is a primer on cyber risk management that delves into some of the quantification and academic literature behind this idea. Nonetheless, it is also intended to be a practical and useful guide for those interested in cyber risk management.

WHY MEASURE CYBER HARMS?

If you have never been hacked, it is hard to believe that it can happen. If you have not lost your business due to cyber-attacks, then these may seem like a nuisance, rather than an existential threat. Most people believe that cyber harms are only virtual, and have no real-world consequences, but this is certainly not the case.

People have lost hundreds of millions of dollars,[2] their entire business,[3] and even their lives due to software bugs.[4] Pacemakers have coding flaws and security failures,[5] trams have been crashed by children,[6] and power turned off to hundreds of thousands,[7] [8] thousands of gallons of sewage have been released,[9] drones diverted,[10] and nuclear enrichment halted.[11] It is essential that people understand that cyber risks may lead to harm: they have ever far-reaching, real-world consequences because computers are continuously being

2 Retrieved from https://www.bbc.co.uk/news/business-19116715
3 Retrieved from https://en.wikipedia.org/wiki/DigiNotar
4 Retrieved from https://en.wikipedia.org/wiki/Therac-25
5 Retrieved from https://cra.org/ccc/wp-content/uploads/sites/2/2015/11/Kevin-Fu-Medical-Device-Security.pdf
6 Retrieved from https://www.wired.com/2008/01/polish-teen-hac/
7 Retrieved from https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack
8 Retrieved from https://www.bbc.com/news/technology-38573074
9 Retrieved from https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill
10 Retrieved from https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident
11 Retrieved from https://en.wikipedia.org/wiki/Stuxnet

put at the heart of the systems that are built in the world (Anderson, Leverett, & Clayton, 2017).

Measurement of harm is at the core of these issues. Without measurement, this goes undocumented and there may be a general feeling that cyber harm does not exist. Clearly from the above-mentioned examples, we know that cyber harms can be real, physical, and pose existential threat, since they impact businesses, civil society groups, and individual people. The first step in understanding the scale of the problem is to either measure or seek measurements that are already in place.

WHAT IS CURRENTLY BEING MEASURED AND WHAT SHOULD BE MEASURED?

Computer Emergency Response Teams, such as CERT.br,[12] have records of cyber incidents, DDoS amplifiers,[13] malicious DNS servers,[14] honeypots[15] and spam. These metrics can be useful for offering a larger picture on the theme of cyber harm, but what other measures are missing? How can more metrics be collected in such a way that they will continue to be useful in the long term?

Box 1 presents seven principles of cyber risk metric construction that can be helpful for managing risks and beginning to quantify them. For example, the question "Are incident counts an effect of the number of incidents or the number of incident responders?" can be solved by skillfully applying the seven principles in overlapping intersection.

---

12 CERT.br is the Brazilian National Computer Emergency Response Team, maintained by the Brazilian Network Information Center (NIC.br), the executive branch of the Brazilian Internet Steering Committee (CGI.br). CERT.br is responsible for handling computer security incident reports and activity related to Brazilian networks connected to the Internet. It is a focal point for incident notification in the country, providing the coordination and necessary support for organizations involved in incidents. Retrieved from https://www.cert.br/stats/

13 A DDoS amplifier is a computer that responds with more data than is sent by the user. Essentially, it must also be open to detours: for example, if I send a letter pretending to be you and subscribing to thousands of free magazines, my one letter is "amplified" and you will be making many trips to the recycling center. Think of it as someone maliciously making you work hard to clean up your mess. Retrieved from

14 A malicious DNS server provides incorrect answers to victim-institution domain name(s), usually financial institutions, e-commerce, social networks and/or well-known domains. Its purpose is to direct users to fake websites. Retrieved from https://www.cert.br/stats/dns-malicioso/

15 A honeypot is a dedicated security computing resource to be probed, attacked, or compromised. Retrieved from https://www.cert.br/stats/honeypots/

BOX 1 - SEVEN PRINCIPLES OF CYBER RISK METRIC CONSTRUCTION

Principle 1: Ratios
It is fundamental that the right data is measured, but also that this is done in a way that allows such measures to continue being useful as new kinds of risks and harm emerge. The method used for measuring cyber risk and the inevitable implications and biases related to this choice are very important and must be taken into consideration. As Eric Jardine (2018) once said, it is important to "mind the denominator." In other words, in keeping count of cyber incidents, we must balance the number of incidents against the size of the team population, or even better, the size of the population of Internet users.[16] [17]

Principle 2: Minding the growth of the denominator
Risk metrics require ratios, and it is important to mind the growth of both the numerator and denominator of such ratios. In this context, when measuring cyber risk, it should be considered that the population is growing in three distinct ways: *(i)* overall, the world population is growing, as is the number of Internet users; *(ii)* the total number of computers of all types is growing – desktops, laptops, mobile phones, Internet of Things (IoT) devices; *(iii)* even the number of computers on the Internet is growing in different ways. There are three reasons for this, also distinct: firstly, more Internet connections are becoming possible daily; secondly, IPv6 addresses – a new form of addresses that are in use on the Internet – are vastly larger than IPv4 spaces;[18] thirdly, we have an ever more dizzying array of top-level domains and DNS entries[19] than ever before. All these factors may contribute to the rapid rise in the total number of incidents. They all form a very dynamic denominator that should be carefully recorded.

Principle 3: Recording work
Aside from keeping measurements with an acknowledged ratio structure, it is also important to have metrics of money, effort, and time. This includes the duration of an incident, the amount of resources applied to this and the number of external parties involved in remediation.

---

16 In considering the number of Internet users, one should be mindful that this includes the vast amount of people that use services through their mobile phones but have no Internet connection at home.

17 A statistical and theoretical foundation of measurements can be found at: https://www.statsdirect.com/help/basics/measurement_scales.htm

18 IPv6 is the most current version of the Internet Protocol. The main reason for deploying IPv6 on the Internet is the need for more addresses because the availability of free IPv4 addresses has ended.

19 A top-level domain (TLD) is the part of a domain that comes after the dot, for example, org or net. A DNS entry is a database that maps human-friendly URLs to IP addresses. When someone types in a URL such as google.com, that entry is sent to an Internet Service Provider (ISP) where it is forwarded to the DNS servers, and then directed to the proper web server, using the corresponding IP address as a label.

Principle 4: Ranking
Sometimes, it is not possible to accurately quantify a risk, or multiple risks. When it is not possible to score something, another possibility is to rank them in an ordering. This can often be accomplished with expert opinion, or discussion groups. A simple ranking of a harm, risk, threat, or impact is often the first step on the path to quantifying the risk.

Principle 5: Decreasing and decommissioning
A good risk metric must be able to both rise and fall. A list of perils should allow items to be removed, as well as added. In practice, this means that when combining measurements into a risk metric or score, basic theoretical work must be done to see that numbers can fall as well as rise. This can be done through a list of criteria to be met before a risk is added to the register, and a list of criteria for removing it from the register. It may return at a later data, which is acceptable, but the main point of risk management is prioritizing the uncertain risks, especially those with the most impact. Certainty can then be added into them where possible, as well as making the best decisions possible.

Principle 6: Beware of average, embrace variance
Averages are a useful shorthand but cannot always be successfully applied to achieve an accurate outcome. When trying to apply an average, it is important to always report variance[20] and to understand what kind of distribution is being studied (for example, if it is a standard, normal distribution).

Principle 7: Recognize biases
Biases exist within all measurements and should be recognized and documented; thus, a good risk practitioner will always ask which biases exist in a metric before they apply it to a decision. It is worth studying both logical fallacies[21] and cognitive biases[22] to understand how they impact measures. Instead of denying a bias, or that a logical fallacy has occurred, one should learn to identify them, document them, and acknowledge when they will or will not be impactful to the task at hand.

---

20 The variance measures the average degree to which each point differs from the mean – the average of all data points.
21 Retrieved from https://yourlogicalfallacyis.com/
22 Retrieved from https://yourbias.is/

COMPLIANCE RISK

One of the first things most organizations address in risk management is their compliance. This is a known risk, and usually with measurable, or at least bounded, consequences.

Being compliant is usually just a matter of creating a good habit, or a procedure that everyone in the organization follows. Auditing or other methods can be used to check compliance regularly as well as to communicate the importance of the risk to others within the organization.[23] A good example is that if an organization processes credit cards online, it must be PCI-DSS compliant, which means, in brief, that it handles credit card and other payment data in a prescribed manner. In practice, this compliance risk is very important, given that cyber criminals in Brazil focus very heavily on credit card fraud. This means that if people's credit card data is taken, it is probably stored or transferred as part of this organization's business.

LEGAL FRAMEWORKS

It is important that organizations check that they comply with local laws and regulations, but also with foreign laws and international standards. They must familiarize themselves with applicable laws, and then consider how their organization runs and what could go wrong for them to fall afoul of these laws. If this is done well enough, they can begin to keep score by measuring the risk, and importantly how much effort it takes to reduce those risks by a measurable quantity. This idea is at the heart of risk management: How much work should be done for how much risk reduction?

Knowing the laws and their penalties is, therefore, very important for understanding the most common data breach risks. In the Brazilian context, the following laws are applicable to most small businesses:

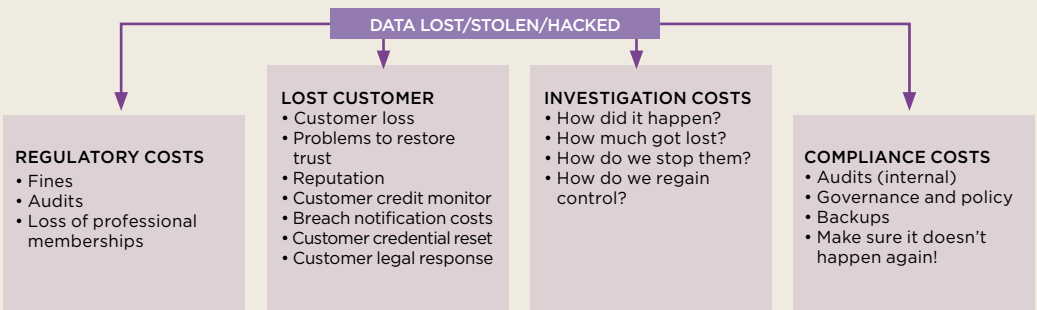
- Brazilian Civil Rights Framework for the Internet (Law no. 12,965);
- Industrial Property Law (Law no. 9,279);
- Software Law (Law no. 9,609);

23 There is a rich literature on managing compliance risks. For example, Romanosky, Ablon, Kuehn and Jones (2017) analyze the contents of cyber insurance policies to understand what they cover and what they do not and learn how they approach risk through the questionnaires they send to potential clients.

- Brazilian General Data Protection Law (Lei Geral de Proteção de Dados – LGDP);
- European Union General Data Protection Regulation (GDPR);[24] and
- Payment Card Industry Data Security Standard (PCI-DSS).[25]

It is important to map how these laws might apply to specific businesses or organizations. For example, consider an organization's customers and the data about them, including how much they pay for this organization. Since this kind of information is likely to be covered by the LGDP, it is important to consider how such data is managed and stored. In this context, what could go wrong and how would it be possible to fix such problems? How much would this cost in comparison to the cost of prevention? If it cannot be prevented, is it possible to reduce the losses through a pre-prepared breach response playbook? These are important questions that need to be addressed by organizations.

HOW DOES LOSING DATA COST MY ORGANISATION MONEY?



SOURCE: PREPARED BY THE AUTHOR.

24 The GDPR is a European law regulation on privacy and protection of personal data, applicable to all individuals in the European Union (EU) and European Economic Area (EEA), created in 2018. It also regulates the export of personal data outside the EU and EEA. The regulation aims to give citizens and residents ways to control their personal data and unify the European regulatory framework.

25 Information security standard for organizations that handle brand name credit cards from the major card schemes.

In this scenario, the first step in managing cyber risk is to find out what laws an organization must comply with. It is also important to consider laws in countries where the organization's customers or suppliers live in, such as GDPR.

BOX 2 – MANAGING COMPLIANCE RISKS

The following checklist can be used as a starting point for managing an organization's compliance risks:

- Making backups of critical data;
  - Online
  - Offline
- Double checking bank accounts and invoices over the phone;
- Training employees about common local scams, and encouraging them to discuss;
- Using antivirus, but understanding that it may not always be enough;
- Forming a cooperative to discuss cyber risks with other small businesses locally;
- Thinking about how your business might function without data or Internet;
- Thinking about how to restore the business from a small amount of data or having to rebuild something that is already running.

The last item is particularly important, since many businesses focus so much on growth and continuing operations that they do not practice rebuilding when things do not go as expected. Lipson and Fisher (1999) emphasize this idea:

> Many businesses have contingency plans for dealing with business interruptions caused by natural disasters or accidents. Although the majority of cyber-attacks are relatively minor in nature, a cyber-attack on an organization's critical networked information systems has the potential to cause severe and prolonged business disruption, whether the business has been targeted specifically or is a random victim of a broad-based attack. If a cyber-attack disrupts critical business functions and interrupts the essential services that customers depend upon, then the survival of the business itself is at risk. (p. 3)

However, spending time and effort planning to rebuild from scratch becomes simpler every time it is practiced. Business continuity drills are useful for many situations, and mostly just involve imagining having to rebuild something from backups, or

old plans. Business continuity is about contemplating and studying events before they happen; therefore, simply spending half an hour a week reading and understanding current cyber risks, then planning to prevent or restore from them is generally sufficient.

LGPD

The new Brazilian General Data Protection Law (Lei Geral de Proteção de Dados – LGDP) was approved in August 2018 and took effect in August 2020. Enterprises that are already GDPR compliant are well on their way to fulfilling LGPD obligations;[26] however, all organizations need to prepare accordingly.

In the context of the LGPD, the next section explains how a qualitative risk assessment can quickly become a quantitative one. To begin with, one should consider that fines for not being compliant with this legislation can be 2% of an organization's revenue and up to BRL 50 million, which already provides a sense of the severity of this risk. Even if the frequency of compliance enforcement and fines are unknown, a principled approach can be used to develop a better risk management program. There are two great principles that can be used in the absence of more data: *(i)* spend up to 37% of the cost of an incident you want to prevent (Gordon & Loeb, 2002); and, *(ii)* if you cannot spend money on the problem, spend more of your time.

As an example, if we consider an organization that handles the data of European citizens as part of its activities, a quantitative risk assessment is remarkably simple. In the worst case scenario, in which it loses a large amount of data, it would cost the organization EUR 10 million or 2% of its global turnover, or if it really impacted individuals' freedoms and rights, EUR 20 million or 4% of its global turnover. While a small business in Brazil is unlikely to see these fines, it is not impossible, and it allows us to start thinking about data protection in the following way: would the organization spend a little amount of money to avoid ever seeing these fines? Or if it cannot afford any extra money, would it spend a little extra time?

How much should this organization spend on data protection for GDPR? 37% of 4% is 1.5% of its global turnover. This

26 More information about similarities between the GDPR and the LGPD available at https://gdpr.eu/gdpr-vs-lgpd/

is a good start for small businesses, generally, and not just for GDPR. That is also remarkably close to the 2% an organization could be fined under LGPD: if an organization is spending on compliance for GDPR, it is also probably very close to compliance for LGDP as well.

These costs can be embedded in the organization's prices, and the practice of digital risk management should be communicated to customers, which is a simple form of reputation management. It is also possible to spend time in basic activities such as removing old passwords, checking log files, upgrading firewalls, and making backups. Alternatively, an organization could spend that time auditing itself and seeing what is and what is not accomplished in the aid of compliance. That could be just 1% of its time, but it needs to be quite a regularly repeated habit, because with this done correctly, if anything at all happened to one's business, one would be able to rebuild it within a few days.

Old business models may now be illegal under LGPD: the new rules may affect an organization's business model as well as how it stores data. For example, if it stores data on private citizens or their spending habits, it should spend the time to understand if it is possible to make that business compliant under the new legislation.

The maximum impact of a GDPR fine is 4% for an egregious breach of data about European customers, more than LGPD, but it is conceivable that an organization could be fined under both legislations at the same time.

Spending on one probably benefits the other, and vice versa; so, organizations do not need to spend 1.3% of their budget on both, they can simply focus on risk mitigations and reductions that impact both. Stating it as simply as possible: **businesses can spend 1.3% of their global turnover, or half an hour per week to avoid fines of up to 4%.**

PCI-DSS COMPLIANCE

There are global regulations for any organization which handles payments, either for themselves or on behalf of others. Their focus is on credit or debit card payments, both online and offline.

While PCI compliance cannot guarantee that an organization would not get hacked and lose its customers' credit or

debit card details, it can certainly protect it from further fines if such an event were to occur. Being compliant in this context simply means adhering to current best practices, which is a significant defense in a court or with regulatory bodies. It means that everything expected was covered reasonably by the organization. Conversely, not being compliant implies that, on top of an incident, an organization might find itself with fines and other regulatory pressures such as audits or payment delays.

How to know if an organization needs to be compliant with PCI-DSS

As stated in the Payment Card Industry Guide,[27] "PCI applies to every business that transmits, processes or stores cardholder information – there are no exemptions." In essence, it is very simple to know whether an organization needs to be compliant with PCI-DSS. Using payment card data of **any** kind, even just to process payments for coffee at the counter, implies that spending a little time thinking of PCI compliance is needed. The good news is most businesses are classified as tier 4, meaning they process less than 20,000 payments a year online or up to 1 million offline, which means the requirements are not very heavy upon them.

If an organization has more money than time, it can outsource these tasks to other organizations who specialize in this. However, using an outsourced provider is not enough by itself, since a self-declaration will be needed, as well as understanding the point of the exercise.

CALCULATING IMPACT BREAKOUT

You want a valve that doesn't leak and you try everything possible to develop one. But the real world provides you with a leaky valve. You have to determine how much leakiness you can tolerate.

ARTHUR RUDOLPH (1996)

The quote that opens this section captures a raw realism that any organization can relate to; it is exactly the same for cyber risk. Since it is not possible to prevent all the bad things that

27 Retrieved from https://www.pcicomplianceguide.org/pci-myths/

can go wrong on the Internet, it is important to figure out how much a cyber risk program can tolerate. Organizations may even strategically alter their tolerance for cyber risk at different times in their life cycle; however, to get to that maturity, one must be able to measure risk.

In relation to calculating the impacts of cyber risk, as previously seen, this task is not particularly difficult for cyber risks in the compliance category. Indeed, many of these fines are precisely calibrated to push organizations to internalize the costs of data breaches, or payment fraud. In other words, where businesses used to avoid responsibility for these events, the regulators are starting to pass on the costs, with the intention that businesses learn to handle the data more carefully.[28]

Although calculating impact can sometimes be as simple as looking up the maximum fines for non-compliance, this approach can be more subtle, or the costs unknown. The first step in any such situation is to make a quick estimation, and ask questions about money, time, and effort. For example, how much would it cost if someone scammed an organization staff into paying them money? One might be tempted to argue that it is impossible to predict this, however, it is possible to focus on minimum and maximum predictions. For example, the minimum might be 0, since it is possible someone scams us, but we are able to inform the bank quick enough and stop the payment. A maximum seems impossible to calculate, but a quick examination of the maximum our bank account has ever held might be an easy start. The further effort is put into this approach, one will begin to see that 0 and our max corporate/bank payments are not equally likely. Putting probabilities around those different amounts may place one well on the way to cyber risk management.

As Hubbard and Seiersen (2016) state, risk quantification is rarely about arriving at a precise number, it is really all about reducing your uncertainty. When an organization has a range of possible impacts for any given cyber risk, and some reasonable confidence around those figures, it can start to examine the four pillars of risk management (Box 3) as different treatments to these risks.

---

28 This kind of phenomenon is heavily documented in the security economics literature, such as Anderson and Moore (2006).

BOX 3 - THE FOUR PILLARS OF RISK MANAGEMENT

1: Avoid risk
Business managers who tend towards this approach are known as risk-averse, and sometimes, that is the right way to run certain kinds of businesses and charities. In other kinds of organizations and businesses, this strategy might prevent innovation or success. In short, risk tolerance can and should be adapted to the core mission of the organization.

2: Accept risk
This is how most people operate in the face of cyber risks. They focus on making the money of the business, and rarely spare a thought about the risks. When they do, they are dismissive of how serious the consequences might be and are reticent to spend time or money reducing their uncertainty.

3: Reduce/restore risk
A good risk manager knows how to ask different people to help them reduce the risks, before accepting them. A brilliant risk manager will also examine not just how to prevent a risk, but how to reduce the impact if it does occur (for example, encrypted data). With cyber risk, restoration strategy is often ignored. Almost all efforts are spent on anti-virus and firewalls (reduction), and very little effort is spent on business continuity plans, incident response plans, and encrypting data (restoration). Note how all these latter treatments assume a risk will happen, but seek to reduce its impact, or restore the business as quickly as possible.[29]

4: Transfer/share risk
Imagine such a tight and vibrant community, and so dedicated to each other that every business who supports your business put a few coins into a jar. This jar would only be opened in case of harm, and if you succeed, you put a little money into the pot for a future business who might be at risk. That is a cooperative of business sharing risks and doing so in a rather creative way. Of course, they could also form an insurance cooperative where every business pays a small fee but get much more than that fee if they are harmed. Insurance does not always have to be provided by giant mega corporations, even small organizations can form a club to share and transfer risk.

TRANSFERRING CYBER RISK

To illustrate cyber risk transferring, consider a scenario where a cyber insurer was to inspect a business that wanted

29 A broad overview of reduction strategies and literature can be found in Gordon, Loeb and Sohail (2003).

to protect 25% of its revenue in case of a breach. The insurer might be willing to take that risk and may even receive a small premium paid by the business. However, the insurer might be willing to pay a much larger amount to the business if there is a breach, more than it can possibly kept in the bank. The insurer would probably have some demands of the business, such as perhaps being compliant with GDPR, PCI-DSS, and LGPD. However, if it were, and passed all casual audits, the insurer would be willing to transfer to himself some of the business' risks for a certain price.

Of course, a local cooperative can do exactly the same thing **without** money. Imagine a small group of businesses who work near each other, agreeing to store each other's backups of data for their business. They could discuss the best practice for how to store the data, and how they all might dedicate a day of their own time to help any other business hit by a cyber-attack. This is also a form of risk transference and sharing, without any money changing hands. In fact, CERTs are a form of cyber risk transference because they protect their constituents with their time.

THE COMMON RISKS AND HOW TO QUANTIFY THEM

Although there are many different cyber risks, the most common ones are explained below. It should be noted that the rare kinds of cyber risks can often also be treated in the same way as the common ones.

DATA LOSS (ACCIDENTAL AND MALICIOUS)

The simplest first step in cyber risk management is having a method for being contacted by external parties which can be as simple as an e-mail address, a requirement under ISO/IEC 27002:2013. More detail is presented below on data breaches, their costs, and responses to help build a robust cyber risk management framework for businesses.

At the lower end of the spectrum, breaches cost varies with the size of the data lost, which is measured in the number of records. For example, if a given business processes 200 credit cards a month, it might have 2,400 credit card details over the last year. As some might be repeated customers, in reality this could be 2,000 records. To keep it simple, if an enterprise loses

10,000 records, it can expect it to have a cost of USD 1,000. This changes slightly at the P8 scale,[30] where losing 100 million records does begin to cost around USD 100 million.

It is easy for a small business to think they have less records than they do. A good starting point is that organizations probably have a record of every employee who has worked for them. Also, many small companies or organizations have much more data than employees. So, when looking for a number of records that an organization would be likely to lose if a **breach did occur**, it can use estimates of the number of customers as a starting point. However, it should be noted that the number of records lost is not a great predictor of cost for mathematical reasons (Cyentia Institute, 2020): a much better approach than the flat cost per record is the mean or geometric mean.

37% of the loss being prevented should be spent on contingency plans; this way, it is worth having two plans, one for the first three days of a breach notification, and one for the next month. The first three days are crucial and can be the difference between losing a lot of money and only losing a little. In fact, the response to a breach can even lead to an **increase** in share price during a crisis if it is as good as Norsk Hydro's.[31]

In the case of a breach, it is important to have a plan for information technology (IT) investigation and response to fix what happened. Plans should also include managing customer communications and enquiries, perhaps even providing fair compensation for any loss. Media response is also crucial at this time both in a brand promotion sense (companies that deal honestly and openly with their incidents usually do not suffer badly in stock exchanges or the court of public opinion). Investor communications or a report to the board might also be critical.

Many of the regulatory frameworks worldwide require a rapid reporting to a regional authority within the first 48-72 hours as well. It is therefore very important to know these regulations, whose job is to make that report and give them any budget/time they need for the tasks.

---

30 Logarithmic scale of breach sizes, released by the center for risk studies which the author is part of, and documented in the book by Coburn, Leverett, and Woo (2018).

31 Hydro was the target of an extensive cyber-attack on March 19, 2019, disrupting operations in several of the company's business areas. More details available at https://www.youtube.com/watch?v=C6MDz-AgQuE

For the longer term, more strategic plans should be considered, such as legal plans, corporate communications, and an increased IT budget to lower the chances of these events occurring again. Many firms specialize in crisis communications and can be a great help during a breach, such as Brazil, that also offers a lot of advice and support through its CERT.[32] It is worth noting that there are important differences in how to handle cases that were accidental, such as leaving data on a laptop in a car that was stolen, and those that were malicious, such as a malicious hacking event where the data was stolen on purpose.

In the first example, it may be the case of opening an investigation, such as putting in a police report, and making a new policy about not leaving laptops in cars; regulators are informed either way, but in the case of a malicious theft of data, it may be necessary to go straight to the CERT,[33] which is likely to be much more helpful than the police if hacking is involved, as the investigations in cyber cases can take months and may never result in clear answers.

Calculating frequency breakout

Figuring out how likely it would be to be hacked is remarkably difficult, because it is subject to a lot of factors such as the capabilities of hackers, the business sector, or the chance of being targeted because a technology happens to be vulnerable. In short, small businesses are unlikely to have a good idea of how probable it is that they will be breached.

However, using pre-done analysis can be extremely useful. Usually, this involves calculating a ratio, known as an incidence rate. For this, there must be a known population as well as knowledge on how many events happen to that population. That could be breaches per company, or ransomware events per person. Usually, these rates have already been calculated, and the details can be quite tricky. For example, with ransomware in 2016, we have prior work that tells us it is around 3% and 4% (Simoiu, Bonneau, Gates, & Goel, 2019; Hull, John, & Arief, 2019). For cyber risk management, one can assume that the year-

32 The publications of CERT are recommended generally. If an incident occurs, they should be contacted directly.

33 Retrieved from https://cert.br/csirts/brasil/

ly chance of being hit by ransomware is roughly between 3% and 4%, unless there is money and time available to dig much deeper.

For breaches, frequency is linked to organization size.[34] If we know nothing about a business, we can assume a breach probability of between 5% and 7% per annum; however, this is wildly inaccurate in most cases, because the number reported is the highest breach frequency when we break down by sector, being the highest for the public sector. If you look at the other sectors, most of them have a breach frequency below 1% (between 0.82% and 0.03%). Simply looking up these data by sector will give a good idea of the frequency of risk for data breach. Similarly, company revenue is a good predictor, ranging from 0.07% for firms earning less than USD 10 million to 75% for firms earning more than USD 100 billion.

BUSINESS E-MAIL COMPROMISE (BEC) AND PHISHING

In practice, business e-mail compromise (BEC) takes many different forms that range from changes to invoices to the use of fake websites, social engineering, via e-mail, or on the phone, and many more tactics. For this reason, mitigating this hazard is never very simple. Multiple risk treatments need to be applied in a way that each one builds upon the successes of the last, assuming that each can also fail.[35]

There is not much written about the frequency of BEC, other than the occasional mentioning of percentage increase or number of incidents. The base rate of businesses in some countries or even globally that are hit by such events seems to go unreported in the literature thus far. Presumably, cyber insurance companies have these figures but are unlikely to share them since this information is the core of their business.

However, reading insurance reports may be insightful and helpful towards understanding risk. For example, one quarter of the 3,300 global incidents in the Beazly 2018 Breach Report were from BEC.[36] This number is only a broad guide and tells

34 More details are provided in Cyentia Institute (2020).

35 An easy conversational introduction to the ecosystem that supports BEC can be found in a KrebOnSecurity interview, available at https://krebsonsecurity.com/tag/bec-scams/. A deeper dive into the more technical details of BEC can be found in the fantastic Trend Micro report (Trend Micro, 2017).

36 Retrieved from https://www.beazley.com/news/2019/beazley_breach_briefing_2019.html

us it makes up a sizable portion of the regular cyber risk. Many papers have been written about how to respond to this kind of risk, with solutions ranging from things a small organization can do, to more global approaches to address the epidemic.[37]

If the proven methods of prevention and mitigation are put into place, how do we monitor and measure their effectiveness within our organizations, or even globally? One simple way that is easier internally than globally is to schedule a phishing test, which can be conducted by a specialized company to carefully measure detection rates.[38] If a hacker sends one thousand e-mails to an organization's employees, trying to gain access, how many will fall on inactive accounts? How many will end up in spam filters and how many will get read? How many will be reported by employees in the correct channel? How many of those will get investigated? How many of the links will be clicked? How many of those clicks might lead to computer compromise? How many might lead to successful social engineering? How many of this final sub-division of those original one thousand e-mails might lead to a costly event, and how costly might that event be? Would it be more costly if we were slow to detect the breach? Carefully quantifying each of these steps and understanding each of the layers of defense – from technical, to human, to detection, to reaction –, is the goal of a good BEC program.

How to calculate efficacy breakout

Once treatment has been applied, how do we know how effective it has been? The simplest way is to test it by trying to get past it. This can be done by someone inside your organization, or a professional ethical hacker or social engineer to try to circumvent risk treatments. The number of attempts they make over the number of successes they achieve is a good way to examine the efficacy of the control. The fact that a

37 Despite being nearly 5 years old, one of the best resources for organizations – small and large – is the London Action Plan. Retrieved from http://londonactionplan.org/wp-content/uploads/2012/12/Operation-Safety-Net-web-version1.pdf

38 There are many organizations that can conduct automated phishing penetration tests/simulations. There are also organizations that can conduct more tailored human designed and bespoke phishing simulations for other organizations. The difference is of course cost, but local organizations should be prioritized, primarily for linguistic and cultural reasons.

control is not 100% effective does not make it useless, unless it is too costly. Rather, it simply means more risk treatment must be carried out so that they apply earlier and later in an attacker's timeline.

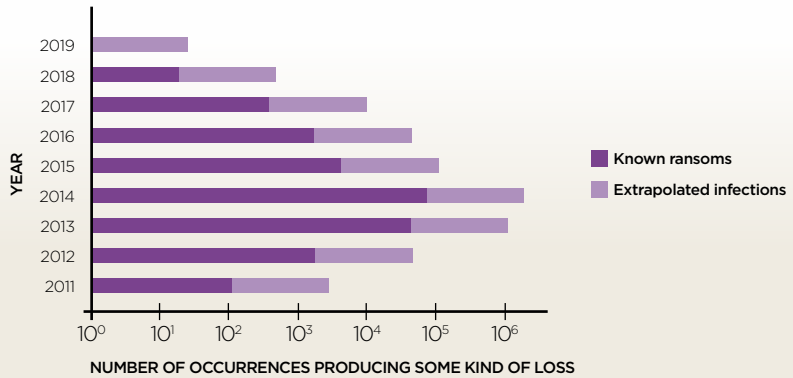
RANSOMWARE

Ransomware is digital extortion, which means that hackers deny you access to your own data or computers. They usually do this by encrypting or deleting the data, and sometimes the latter are called wipers. Occasionally, ransomware gangs threaten to publish the data, or take your website offline with a DDoS (denial of service), but they all try to demand money, often through bitcoin, but also through other cryptocurrencies or online store gift cards. There are many ransomware gangs, and the impact they have had over the last 10 years is quite staggering on both small and large businesses.[39]

In the context of small businesses, what can they do in such an event? How many of them are affected every year? It is possible to estimate the total number of infections based on the number of ransoms paid, and the willingness to pay ratio discussed above. By applying the willingness to pay ratio and multiplying the number of ransoms known to have been paid, we can get a rough estimate of the total number of infections, even where ransoms were not paid (Chart 1). We must acknowledge there is a sampling delay introduced by how the data is gathered, so we do not realistically believe that the number of attacks is falling so sharply. This is an application of both the principle of ratio and the principle of acknowledging bias. The data is useful to put a lower bar on the number of infections, but it should not be used to conclude trends in recent years because of the delay in data acquisition.

39 The author's own company runs a database of a decade of recorded ransoms so insurance and risk companies can more accurately calculate the risk of ransomware. More information available at https://billing.concinnity-risks.com/

CHART 1 - LOWER BOUND ESTIMATE ON RANSOMWARE OCCURANCES



SOURCE: PREPARED BY THE AUTHOR.

In summary, Chart 1 shows that for every ransom paid, we can expect to see another 25 infections that cost money to the organization, even though they did not pay the ransom.

Most businesses cannot function without computers, or without the data they contain – from phone numbers and e-mails to bank account numbers and digital manufacturing. If this data was suddenly encrypted or deleted, it would be very difficult to keep working.[40]

There are people constantly working around the world to write cures to these digital infections, known as decryptors. They do not always exist or work properly for all ransomware families, so what does a small business have to do in face of this incident? Plans must be in place for risk reduction and impact reduction.

In the category of preventative measures and risk reduction, there are very traditional and well-known methods. Anti-virus can stop a lot of the older and more common types of ransomware, but not the freshest, newest types. It can be useful for key business workers to set up an old lap-

40 If such a situation occurs, it is worth visiting the following website https://www.nomoreransom.org/, which allows the upload of ransom notes in attempt to identify the gang or type of ransomware. The website offers tools that could be used to decrypt data without paying the ransom. Guidelines are available in many languages, and it is a very helpful first place to visit.

top in exactly the same way they set up a new one and keep both capable of accessing e-mails, invoicing, and timesheets. Some people find this easier by logging in once a month to that computer and seeing if they can still work from it without too much difficulty; if they cannot, then they should update it. This simple exercise is helpful for both learning our dependence on technology, but also for indicating what is most crucial for backups and restoration plans. The advantage of this approach is that this computer forms a base of operations from which it can potentially rebuild. It is crucial though to keep this computer turned off most of the time, and ideally at a different place other than where the business is located. This is because when ransomware strikes, it tends to infect every computer on the same network and of the same type. After an incident, both internal and external communication are key. Externally, information must be conveyed to customers, to the press, to CERTs, insurers, and investors. The response to Norsk Hydro ransomware incident provides important lessons, as does Maersk's:[41] both organizations not only rebuilt portions of their companies from scratch, but also managed to convey a sense of resilience and calm during an existential crisis and have rightly become role models of crisis management during cyber-attacks.

Furthermore, insurance products specific to ransomware can be purchased, and they often come with a package of assistance when such an event occurs. They also require businesses to take several measures in order to protect themselves before selling the insurance.

The costs of ransomware clean-up are much more expensive than the ransom asked for, which is why the criminals make money. If it were possible to clean it up with low-cost businesses, they would have no leverage. That is why organizations should all be focusing on being able to restore their computer systems quickly from scratch **before** a cyber event occurs. If it is possible to restore a computer and data for any part of an organization's business for less than what it earns per month, then it can significantly remove the leverage for the extortion.

41 Details on lessons learned after the cyber-attack suffered by Maersk and on how they were applied within Maersk are available at https://www.youtube.com/watch?v=wQ8HIjkEe9o. See also footnote nº 31.

Another problem with paying the ransom is that it does not remove the cost of clean-up. The fact remains that an organization has been hacked, it must report a breach, and even if someone gives it the key to get their data back, it must figure out how they got in and kick them out again. Sometimes, the decryptors do not work properly, and there is still much work to do even if the ransom was paid. So, it is much better to plan for an incident where a business is locked out of all computers and rehearse with its team how it would respond.

THE UNIQUE RISKS CIVIL SOCIETY FACES, DOCUMENTS, AND OFTEN THWARTS

Most of the risks and harms described up until now are primarily a problem for businesses, but they also affect civil society groups, non-profit or charity organizations. However, there are specific risks that business does not face, but the latter organizations do. From stalkerware to romance scams, to targeted phishing attacks, to politically motivated leaks, and even consumer rights in a technology setting, civil society has faced decades of cyber risks that are often underestimated and under reported.

- Stalkerware is the name given to apps installed on phones to track people. Primarily, it shows up in gender-based abuse or intimate partner violence settings. Some aspects of it fall under the categorization of coercive control, as it sometimes appears in the academic literature.[42] Three aspects of this phenomenon that deserve more attention is how much money these companies are making, how to apply LGDP to protect impacted persons, and for all organizations (including businesses) to realize the impacts intimate partner violence and tech abuse have on their employees.
- Romance scams are a budding cottage industry on the dark web forums, with many tutorials about how to se-

42 A fantastic overview of the issue can be found as documented by the Citizen Lab's report, *The Predator in Your Pocket*: *A Multidisciplinary Assessment of the Stalkerware Application Industry* (Parsons et al., 2019). A much broader and deeper program of research on gender and IoT is ongoing at University College London (UCL) under the direction of Dr. Leonie Tanczer (Lopez-Neira, 2019). More information available at: https://tspace.library.utoronto.ca/handle/1807/96320

duce and romance people so that you can con them out of money, turn them into money mules for laundering your money, or both at the same time. The tutorials often come with places you can buy illicitly acquired intimate pictures, so that you may portray yourself to be someone else. This phenomenon is also known as e-whoring,[43] and readers new to this should note how there are many victims in the ecosystem, from the people whose intimate photos are stolen or conned out of them, to the financial fraud, to the emotional damage of believing in a false romance, and the extra work a victim must do to disentangle themselves from the money laundering accusations.

- Targeted phishing attacks try to trick people into entering their passwords or credentials into websites designed to look like others they use regularly. The targets of such attacks are often people whose work is politically sensitive: journalists, activists, community organizers. Once the credentials are known, they are used in the original websites to gather as much information as possible. Sometimes, they are also leaked to wider audiences. As if being targeted and having one's mail read and released is not traumatizing enough, a worrying new development has unfolded in recent years: the leaks are strategically altered and changed to suit the agenda of the leakers. If most of the leak is factually accurate, and only some of it is false, it is often swallowed whole by the public. This leads the victims of such attacks to exhaust themselves in fighting the misinformation about them and avoiding the dangers associated with such.[44]
- Internet censorship and outages are unfortunately common too. In some cases, they last for years[45] and can even be targeted at particular language groups.[46] The ill effects are documented in a variety of ways,

43 This phenomenon is documented by Hutchings (2019) with a much deeper understanding.

44 A thorough example of this kind of phenomenon is documented in *Tainted Leaks: Disinformation and Phishing With a Russian Nexus* (Hulcoop, Scott-Railton, Tanchak, Brooks, & Deibert, 2017). More information available at: https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

45 Retrieved from https://en.wikipedia.org/wiki/Block_of_Wikipedia_in_Turkey

46 Retrieved from https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

from mental health effects to educational inequality. Even the economic impact on a region can be significant,[47] leading to the many other problems that wealth inequality produces.

- The Internet of Things (IoT) brings with it a very complicated policy dilemma. In its simplest form, this is a slow-moving collision between two philosophies: the first is the idea that software should carry no liability; the second is that consumer rights and product safety are built upon liability. The problem becomes ever more exacerbated the more that the IoT blends into our everyday existence. As microchips enter more and more things, the cost to repair them goes up, but they also stop working when the company that built them goes bankrupt. In addition, the physical damage microchips can cause becomes increasingly obvious. The cost of the impact software quality failures is not simply virtual, although most of society still thinks it is. People working with software controlling the electric grid have been always aware of the enormous potential cost of failure of a tiny bug, but it takes the dawning realization of billions of people that their cell phones are spying on them to understand how this will inevitably lead to software liability.[48] Holding technology companies accountable for harm produced by their products has barely begun but has a deep underlying ability to change the behavior of large corporations.
- Algorithmic bias, usually in the form of racism or sexism, is also a problem. We must be clear that the bias can be in the algorithm itself but can also be embedded within the collected data in the first place. So, even a well-intentioned researcher using what could be considered a neutral algorithm and research methodology can suddenly discover he or she has built a racist or sexist system. As an example, if the dataset was gathered only from men about their salaries, then it necessarily will not take into

47 Retrieved from https://www.internetsociety.org/policybriefs/internet-shutdowns

48 A deeper overview can be found in Leverett, Clayton and Anderson (2017). It would be wise for consumer rights groups to join the debate and get a technologist on staff to help the lawyers.

account the distribution of women's salaries. Thus, any inferences it makes from such data will be highly likely to exhibit a sexist result.[49]

In this section, we have not focused so much on quantification of the risks for two reasons. Firstly, many of these risks are not operational risks to civil society groups, although this is the case for some. In other words, they do not threaten the organizational integrity itself, but rather, they are risks to the people a civil society serves. Thus, quantification of these risks would be conducted very differently, and much more effectively by those organizations themselves. Secondly, these studies are still nascent, and the numbers are not being systematically gathered. Of course, a civil society group could start that process now, and make great progress into documenting these harms – as well as many others – and building an evidence-based policy around it.

EXAMINING RISK TREATMENTS

Risk treatments for cyber harms are diverse and, therefore, cannot be all listed here with accuracy. However, what is important is to recognize the broad themes in the different treatments, as well as benefits, side effects, and counterproductive traps.

Firstly, it is helpful to group treatments into two categories: those that help us prevent harm, and those that help us reduce the impact if it does occur. Some treatments will of course help in both cases, and that is a benefit too. The point is that a risk that is frequent, with lower but repeatable harms, is best dealt with by prevention. Risks that are less frequent but deeply harmful may not be possible to prevent, but much can be done to limit the severity of the event.

To capture this more concretely, it is useful to discuss natural disasters for a moment. We can examine them with three things in mind: can they be predicted or prevented? Can anything be accomplished within the window of prediction? Can the impacts be reduced?

Earthquakes cannot be predicted in a long-term sense, or rather we know they will occur, but we cannot be accurate about when they will occur. They cannot be prevented as an event, but the effects they have on buildings or people can be reduced.

---

49 This topic is documented meticulously by Joy Buolamwini's Algorithmic Justice League, and it deserves much more space than we can give it in this document. Retrieved from https://www.ajlunited.org/library/research

There are warning systems for imminent earthquakes, but these are provided only a few seconds before an event, which is not enough time to accomplish anything to save lives. However, long-term planning can reduce their impact, such as improved building codes to make buildings safer. Now consider floods: although they cannot be prevented (decarbonizing society notwithstanding), the warning systems can sometimes give us notice days in advance and evacuations can save lives. This can also be combined with long-term flood defenses distributed across regions to reduce the impacts. Finally, resources can be provided to help rebuild communities after flooding has hit an area.

The key point is that there is an intersectional quality to how we design our response to these issues that is defined by *(i)* the prediction/warning time window, *(ii)* the amount of measures that can be taken before an event, and *(iii)* the amount of measures that can be taken after an event. The issue is not to choose between prevention and impact reduction, but to do both in the right proportions. It is also important to know – in the natural disaster examples above – how some treatments are centralized (warning systems), and others are decentralized (building safety or flood defenses). Is it possible to achieve the same things in cyber risk? Some solutions such as VPNs and two-factor authentication must be centralized, but other solutions, such as phishing training, can be decentralized. Examining these variations as each risk is studied can help organizations frame their responses and use whatever resources they have more optimally.

JOINT MITIGATION EFFECTIVENESS

Some defenses solve more than one problem, which is a more efficient and cheaper approach. Focusing on these first can enable organizations to find some mitigations such as backups to help them in case of a ransomware attack, or an earthquake or flood. That is precisely the effect we should be focused upon, though there may be other risk treatments that interleave with each of those risks individually.

Cyber insurance for risk leftovers that cannot be treated

After having attempted all other risk treatments that are practical, efficient, and correctly priced for risk reduction, there will be still some residual risks left. Simply accepting the residual

risk and moving on may be tempting, but there remains the option of risk transfer. When all easier options are exhausted, cyber insurance can be used to cover risks if the organization does not know how to treat, manage, or mitigate them.[50]

Buying insurance is not the only alternative. Cooperatives can be created, as it is possible to create insurance pools or insurance captives. There are many ways of self-insuring. For example, a group of businesses can form an insurance cooperative, mutual, or pool.[51] They put aside a little money each month or year, and agree to give some portion of it to anyone hit by a cyber-attack or technological accident. In such a scheme, they can "pool" their resources so that what would be prohibitively expensive for an individual business becomes viable by dividing the risk amongst many. This also has the advantage that while one organization might not be able to afford a full-time security professional, a group of businesses might. Thus, every business gets a timeshare of good security and privacy practices, even though as small businesses they might not be able to afford them.

Another alternative is the construction of an insurance captive.[52] At the end of the day, you are either insuring yourself against risks, or transferring some risk to third parties. Of course, it is also possible to mix and match the strategies listed above to match the level or risk a business is exposed to or has an appetite for. For example, an incident response plan may be in place that projects costs in the first three days, and triggers insurance policy if it looks to exceed a threshold planned by the board in advance. To do that means having begun to measure cyber risk in a repeatable and useful fashion. It means layering risk treatments one against another, improving their efficacy through an interlocking set of policies, responses, and prevention mechanisms. That, at the core, is risk management.

---

50 Romanosky et al. (2017) published a comprehensive paper showing the range of policies available and what they cover. This document also gives a sense of the cost of this solution, and how much the policies deliver when they are activated. An actuarial and research-driven perspective is offered in Marotta, Martinelli, Nanni, Orlando and Yautsiukhin (2017).

51 Retrieved from https://www.insuranceopedia.com/definition/1383/cooperative-insurance

52 Retrieved from https://www.captive.com/news/2018/08/08/what-is-captive-insurance

CONCLUSION

This paper addressed what makes a good cyber risk metric and presents a lengthy discussion on why measures are needed. Useful principles for cyber risk metric construction were also documented, towards the quantification of the large variety of cyber risks.

Despite the wide range of existing cyber risks, an organization should name and list the known cyber risks faced by them. Once named and listed, the risks should then be adequately measured. Equally important is improving the data collection methods used to manage these risks: when collecting data, one should be mindful of ever increasing or decreasing numbers and applied averages. Additionally, while it is important to measure the work that is done, we should not confuse that with risk reduction. Only when the frequency or severity of a risk is reduced, have we measured some element of risk. The effort applied to achieve that risk reduction is what needs to be improved.

In terms of risk measurement, there are important aspects to watch out for. The first relates to the fact that when you gather metrics to represent an economy, it becomes a game for people, and ceases to be a metric (Goodhart's Law). For example, if we reward incident responders by the number of incidents they work, they will rightly start splitting incidents into smaller pieces to record them as different incidents. There is nothing wrong with this, as they are simply doing the same work with a different recording strategy, but it would change everything about what your risk metrics reflected.

The second concern is another incentive design challenge, where the goal is to encourage the **reduction** of risk, but a poorly chosen metric incentivizes **recording** work instead. For example, many risk teams slowly drift towards documenting compliance and the work it requires, rather than continuing to innovate cyber risk. There is nothing wrong with documenting the work, in and of itself, if the risk team stays focused on risk reduction, and innovations towards achieving it or measuring it. If we rewarded ever larger efforts, without documenting risk reduction, we are incentivizing the wrong thing. This is a classic failure of compliance risk departments everywhere.[53]

53 This is documented extensively in the excellent book *The Failure of Risk Management: Why It's Broken and How to Fix It* (Hubbard, 2009).

It is acceptable to be wrong with figures and metrics and improve over time the construction and collection of risk metrics. It is much better to start with an estimate and improve than to make decisions about risky things without the support of evidence. Good risk management teams can handle both uncertainty and biased data, but it is important to give them as much information as possible.

As metrics improve information supporting risk decisions, it improves risk management practice. Yet, there is also hard work to be done to improve organizational risk postures. In other words, they prevent more bad things happening, and they handle them better when they do happen. Another crucial element is to acknowledge and discuss a diversity of risk tolerance. One business might need to take more risks than another to achieve its strategic objectives. For example, a bakery may have a much lower risk tolerance than a search and rescue team. The search and rescue team must **necessarily** take risks to their health and safety in the daily work they do to help others. Though it might amuse the bakers to note that historically they were a riskier profession that improved over time[54] through risk management.

Improvements in the efficiency and effectiveness of risk treatments are the lifeblood of any risk management, so measuring and improving them over time is key. If an organization never learns from its own history, particularly in risk, it will end up poorly managing risk. If there is a vibrant, diverse, and innovative risk team, continually finding new characteristics of cyber risk, then an organization has a hope of surviving the challenges of the next few decades.

Risk reduction is not pursued alone, and many organizations improve their risk management by talking about it or sharing it. There are many, many, organizations over the world dedicated to teaching about risk or sharing risks between wider groups. It is valid to choose one, because the main point is simply to never walk alone.

The most damaging phrase in the language is: "it's always been done that way."

GRACE BREWSTER MURRAY HOPPER (1976)

---

54 Retrieved from https://hughesenv.com/history-of-combustible-dust-explosions/

REFERENCES

Anderson, R., & Moore, T. (2006, October 27). The economics of information security. *Science,* 314(5799), 610-613. doi 10.1126/science.1130992

Anderson, R., Leverett, E., & Clayton, R. (2017). *Standardisation and certification of safety, security and privacy in the 'Internet of Things'.* Luxembourg: European Union. Retrieved from https://doi.org/10.17863/CAM.35286

Coburn, A., Leverett, E., & Woo, G. (2018). *Solving Cyber Risk: Protecting Your Company and Society* (pp. 34-40). Hoboken, NJ: John Wiley & Sons.

Cyentia Institute (2020). *Information Risk Insights Study (IRIS 20/20). A Clearer Vision for Assessing the Risk os Cyber Incidents.* Retrieved from https://www.cyentia.com/iris

Gordon, L. A., & Loeb, M. P. (2002, November). The Economics of Information Security Investment. *ACM Transactions on Information and System Security,* 438-457. Retrieved from https://dl.acm.org/doi/abs/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM 46*, 3, 81-85.

Hubbard, D. W. (2009). *The failure of risk management: Why it's broken and how to fix it*. Hoboken, NJ: John Wiley & Sons.

Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk*. Hoboken, NJ: John Wiley & Sons. Retrieved from https://www.wiley.com/en-us/How+to+Measure+Anything+in+Cybersecurity+Risk-p-9781119085294

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science, 8*(2). Retrieved from https://www.researchgate.net/publication/331046766_Ransomware_deployment_methods_and_analysis_views_from_a_predictive_model_and_human_responses/fulltext/5c6300f2299bf1d14cc1e663/Ransomware-deployment-methods-and-analysis-views-from-a-predictive-model-and-human-responses.pdf

Jardine, E. (2018). Mind the denominator: towards a more effective measurement system for cybersecurity. *Journal of Cyber Policy, 3*(1), 116–139.

Lipson, H. F., & Fisher, D. A. (1999). *Survivability — A New Technical and Business Perspective on Security.* Retrieved from https://www.researchgate.net/publication/2454026_Survivability_-_A_New_Technical_and_Business_Perspective_on_Security#read

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review, 24*, 35-61.

Payment Card Industry Data Security Standard (PCI-DSS). (n.d.) A*pproved Scanning Vendors*. Retrieved from https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

Payment Card Industry Data Security Standard (PCI-DSS). (n.d.) *Attestation of Compliance*. Retrieved from https://www.pcisecuritystandards.org/document_library?category=saqs#results

Payment Card Industry Data Security Standard (PCI-DSS). (n.d.) *Completing Self-Assessment*. Retrieved from https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). *Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?* Washington D.C., VA: Rand, 38. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929137

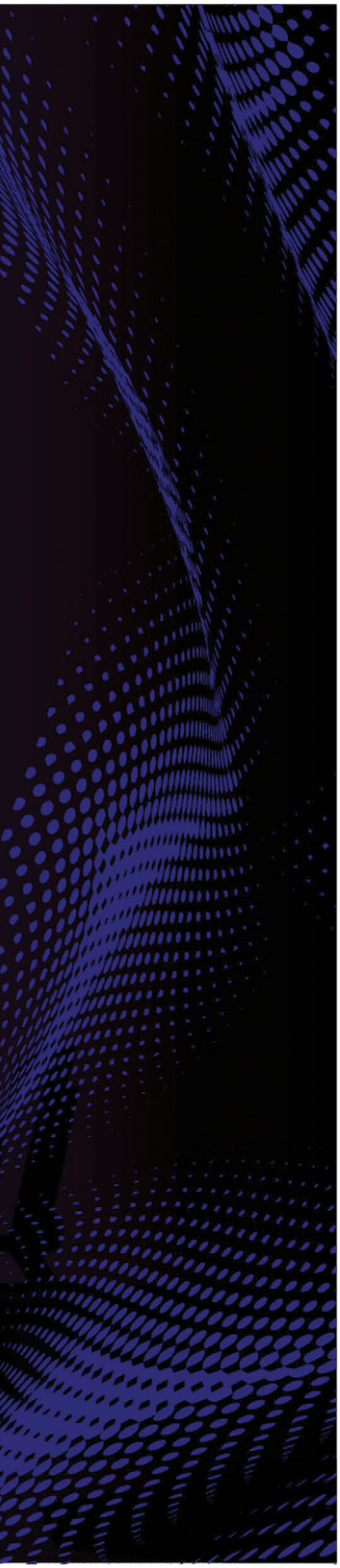
Simoiu, C., Bonneau, J., Gates, C., & Goel, S. (2019). I was told to buy a software or lose my computer. I ignored it: A study of ransomware. *Fifteenth Symposium on Usable Privacy and Security*. Retrieved from https://www.usenix.org/conference/soups2019/presentation/simoiu

CHAPTER 3

Where to invest to reduce risk: A depiction based on reported security incidents and on data from sensors and external sources compiled by the Brazilian National Computer Emergency Response Team/CERT.br

Cristine Hoepers[1]

1 General Manager of CERT.br|NIC.br, Bachelor's Degree in Computer Sciences from the Federal University of Santa Catarina (UFSC) and Doctorate Degree in Applied Computing from the National Institute for Space Research (*Instituto Nacional de Pesquisas Espaciais – INPE*).



INTRODUCTION

In most fields of knowledge, ranging from economics and health to software engineering and development, the Pareto Principle[2] is a relevant concept. In simple words, it states that 80% of the results are due to 20% of the actions. Applying this principle to problems means that probably 80% of these could be resolved by fixing 20% of the mistakes that led to them.

This perception is very important, because we always tend to focus our efforts on that which is new and seems to be more "serious." Thus, we fear airplane crashes more than traffic accidents, even though the latter has a much higher statistical risk of happening.

In relation to attacks on Internet-connected systems, the media and managers focus very strongly on new attacks, such as espionage or cyber war, which exploit complex vulnerabilities or have political motivations. However, in the day-to-day life of organizations, it is much simpler problems with well-established solutions that are the source of most of the successful attacks, as we will see in the analyses in this article, based on data from attacks and incidents observed by the Brazilian National Computer Emergency Response Team (CERT.br).

Considering this scenario, one can argue that three measures could reduce the security incidents reported to CERT.br by at least 80%. The measures are as follows:

1. **Keep all software (operating systems and applications) updated.** In other words, always install and use the latest version of the software with all the updated security features. This holds true for computers, mobile phones, tablets, and the Internet of Things (IoT).
2. **Harden all systems and devices.** In other words, disable all unnecessary services on devices, change all the standard passwords, configure all the services exposed on the Internet to tighten protection, constantly revise the setups, and conduct periodic checks to verify if measure 1 is being followed.

2 Retrieved from https://en.wikipedia.org/wiki/Pareto_principle

3. **Improve identification and authentication processes for logging in to services and systems.** This implies education on password management, with a focus on non-reuse of passwords, and tailoring of all systems and accounts to not only use passwords for authentication purposes. That is, implement and use multiple authentication factors for all services (corporate services, social networks, banks, or any other services).

If the Pareto Principle also applies to the reduction of attacks on the Internet, why are we still facing a scenario with so many vulnerabilities and successful attacks? Why do data leaks grow non-stop? Why is it so difficult to improve this scenario and achieve the desired healthy ecosystem?

This analysis will address the national scenario based on data collected by CERT.br. The data includes incidents reported voluntarily by users and systems administrators, data collected by CERT.br sensors and data collected by international organizations and informed to CERT.br. The conclusion will present some thoughts on the complexity entailed in the implementation of the three measures in a scenario where the Internet of Things is growing significantly, as indicated by data from the ICT Households survey.[3] The cultural perception that everyone must participate in the construction of a healthier Internet has still not permeated society.

DATA SOURCES USED FOR THIS ANALYSIS

The Brazilian National Computer Emergency Response Team (CERT.br), maintained by the Brazilian Network Information Center (NIC.br), is the center that deals with computer security incidents on a nationwide level. It is the organization to which security incidents in Brazil are reported. The constituents to whom CERT.br provides services include all the networks that use resources allocated by NIC.br; that is, all the networks with IP addresses or Autonomous System Numbers (ASNs) allocated to Brazil or that have domains registered under ccTLD .br.

3 The number of people who use TV sets and mobile phones to connect to the Internet increases every year. From a security perspective, the characteristics of mobile phones are more similar to the characteristics of IoT devices than computers. ICT Households – 2019, Individuals, Internet users by devices used (*TIC Domicílios – 2019, Indivíduos, Usuários de Internet, por dispositivo utilizado*), https://cetic.br/pt/tics/domicilios/2019/individuos/C16/

The strategic objectives of the activities conducted by CERT.br are to increase security levels and the treatment capacity of incidents related to users and networks connected to the Internet in Brazil, contributing to the Internet's increasing and adequate use by society. To achieve these objectives, the team undertakes various activities, two of which contribute to the production of data on the status of cyber threats in the national Internet sphere: handling of security incidents involving any national networks – to provide coordination and support in the incident-response process –, and attack trend analyses.

To enable such analyses, CERT.br works with other kinds of data, in addition to data on the characteristics of reported security incidents. It also works with data on attacks that have been observed in the national sensor network (*honeypots*) that it maintains;[4] and with data on threats in the Brazilian Internet space that are observed by global projects on measuring threats and shared with CERT.br. Below is a discussion on the types of data, their characteristics, and limitations.

REPORTS ON SECURITY INCIDENTS RECEIVED BY CERT.br

A Computer Security Incident Response Team (CSIRT) is an organization responsible for receiving, analyzing, and responding to reports and activities related to security incidents in computers. A CSIRT normally provides services to a clearly defined community, which may be the entity that maintains it, such as a company, a government body, or an academic organization. A CSIRT can also provide services to a bigger community, such as a country, a research network, or to clients that pay for its services.[5]

A security incident can be defined as any confirmed or suspected adverse event related to the security of computer systems or computer networks. Some examples of security incidents are: attempt to use or unauthorized access to systems or data, attempt to make services unavailable, modifications in systems (without the knowledge or previous consent of the owners) and non-compliance with security policies or established use policies of an institution. CERT.br is a CSIRT with

4 Distributed Honeypots Project. Retrieved from https://cert.br/projetos/
5 CSIRT FAQ. Retrieved from https://cert.br/certcc/csirts/csirt_faq-br.html

nationwide responsibility and acts as a CSIRT of last resort. It is the contact point in the country to facilitate coordinated cooperation among organizations involved in an incident, whether they are the origin or target of attacks. In other words, it is a CSIRT to which anybody can resort to in case of incidents involving networks allocated to Brazil.

In this context, CERT.br is quite flexible in terms of defining what is a security incident that will be treated by the team. It receives reports on different activities in devices or in networks that could threaten the security of its constituents' computer systems. Once CERT.br receives a report, it starts a process referred to as Incident Management.

Computer Security Incident Management is a set of services that are vital to help the constituents of a CSIRT deal with an attack or an incident. These services include not only the collection and assessment of information contained in the incident reports, but also the analysis of other relevant data, such as technical details and related artifacts. More specifically, CERT.br provides the following services that are part of the Incident Management process:[6]

- Provide support to the recovery process and to the analysis of attacks and compromised systems;
- Establish collaborative work with other entities, such as other CSIRTs, companies, Internet access and service providers, and backbones;
- Maintain official statistics on treated incidents and on complaints of spams received.

Official statistics on incidents treated by the team have been maintained since 1999 and are found on: https://cert.br/stats/incidentes/. As previously pointed out, CERT.br receives voluntary reports from a variety of constituents, ranging from end users to systems and network administrators, from a wide variety of sectors of all sizes. To allow categorization per type of attack and maintain the comparability among data collected over the 21 years during which the statistics have been available, the team decided to specify categories of attacks and group them under most significant types of attacks. The categories under which the incidents are classified are as follows:

6 About CERT.br, https://cert.br/about/

- **worm**: reports on malicious activities related to the automated process that spreads malicious codes through the network;
- **dos (DoS - Denial of Service)**: reports on denials of service, for which the attacker uses a device or a set of devices to shut down a service, a computer or a network;
- **invasion**: a successful attack that results in non-authorized access to a computer or to a network;
- **web**: a type of attack that specifically aims at compromising web services or defacing web pages;
- **scanning**: notifications of computer network scans with the objective of identifying which computers are active and which services are being made available by those computers. Scanning is widely used by attackers to identify potential targets, as they allow them to associate potential vulnerabilities with the services enabled in a device;
- **fraud**: according to Houaiss, a Brazilian Portuguese dictionary, fraud is "any cunning, misleading act in bad faith, with the purpose of harming or deceiving someone, or of not performing a specific duty; deceit." This category includes reports of fraud attempts; that is, of incidents in which an attempt is made to obtain some kind of advantage.
- **other**: reports of incidents that do not fit under the previous categories.

In addition, details on which types of scanning are more frequent are also specified for each year of the series. The scans, although not a successful attack, are an indication of which services are most sought after by attackers and highlight where the most exploited vulnerabilities are located.

NETWORK OF DISTRIBUTED HONEYPOTS MAINTAINED BY CERT.br

CERT.br maintains the Distributed Honeypots Project, a distributed network of low interaction honeypots, in Internet IP addresses in Brazil. The objective of this project is to increase the capacity to detect incidents, correlate events and identify attack trends in Brazil.[7]

7 Distributed Honeypots Project. Retrieved from https://cert.br/projetos/

A honeypot is a dedicated security computing resource to be probed, attacked, or compromised. In low interaction honeypots, tools are installed to emulate operating systems and services with which attackers will interact. This way, the actual operating system of this kind of honeypot must be installed and set up in a safe manner to minimize the risk of compromising the system.[8]

The main advantage of a honeypot is the fact that it is installed in such a way that the traffic attracted to it is, by definition, anomalous or malicious. Therefore, theoretically, it is a security mechanism free from false positives. It provides highly valuable information in volumes that are much lower than those of other security mechanisms, such as the Intrusion Detection System (IDS). It is important to point out that a honeypot is only able to observe the traffic directed at it, and it is not a mechanism that uses traffic inspection.

The importance of a honeypot is based on the fact that everything that is attracted to it is suspicious or potentially malicious. Its application depends on the result that is to be achieved. Normally, the use of low interaction honeypots is associated with the following objectives:

- detect internal attacks;
- identify scanning and automated attacks;
- identify trends;
- collect attack signatures;
- detect compromised computers or computers with setup problems;
- collect malicious code.

In the Distributed Honeypots Project, CERT.br uses low interaction honeypots to detect scanning, automated attacks, malicious codes and compromised computers or computers with setup problems. The following activities are developed to achieve such objectives:

- A distributed network of low interaction honeypots is maintained to cover a reasonable amount of space of IPv4 Internet addresses in Brazil;

8 Honeypots and Honeynets: Definitions and Applications (*Honeypots e Honeynets: Definições e Aplicações*), CERT.br. Retrieved from https://cert.br/docs/whitepapers/honeypots-honeynets/

- Development of a system that, on a daily basis, notifies the incident response teams (CSIRTs) of the networks responsible for originating attacks on the honeypots;
- Official statistics are maintained as follows:
    - Daily charts of network traffic flows directed at all honeypots;[9]
    - Annual statistics and analyses of the most frequent attacks on the honeypots maintained by CERT.br.[10]

INDICATORS RECEIVED FROM EXTERNAL DATA SOURCES

As mentioned previously, CERT.br is the national CSIRT of last resort. As such, it is qualified to receive information from international entities that map malicious activities and vulnerable systems on the Internet. This information is related solely to the IP address space allocated to Brazil and is part of sources of information used by CSIRTs from all around the world for the purpose of proactively detecting network security incidents.

CERT.br receives data from several organizations. The most relevant for this analysis, however, is the data received from the Shadowserver Foundation[11] and from Shodan.[12] Data from the Shadowserver Foundation includes data on vulnerable or infected devices collected by passive sensors and data from scanning carried out in the entire IPv4 address space. Shodan is a search engine that lists Internet of Things (IoT) devices, with a focus on the search for vulnerable devices exposed on the Internet.

SCENARIO OF ATTACKS OBSERVED IN BRAZIL'S INTERNET SPACE

In this section, we will look at the data that can be observed in the sources CERT.br has access to, beginning with incidents reported to the team. This will be followed by data from honeypots and then by data from external sources.

---

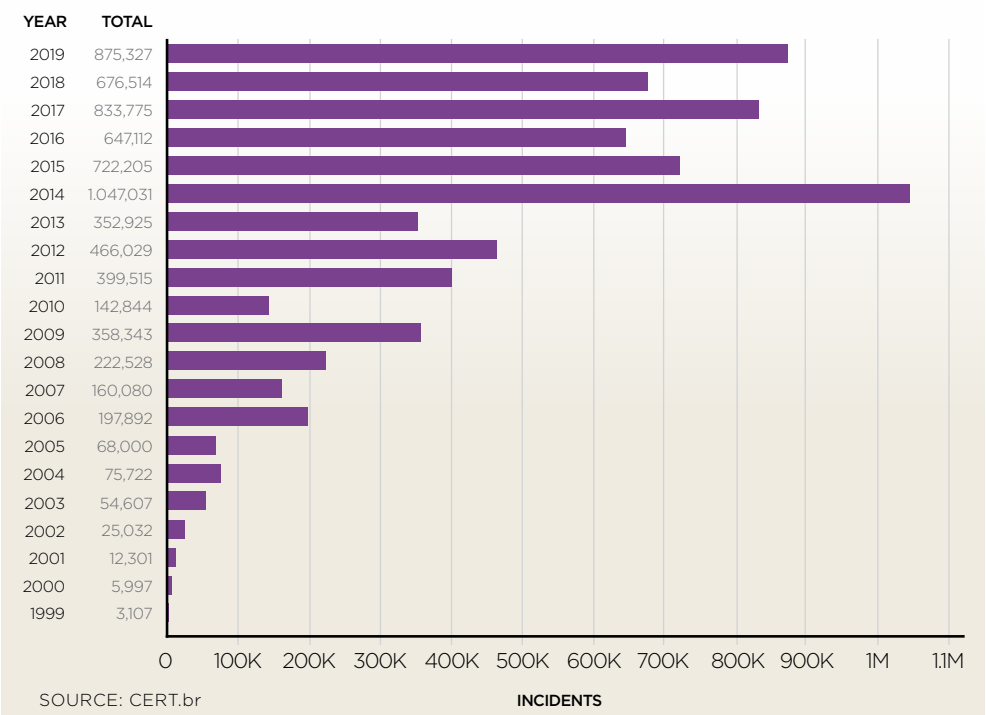
9 Retrieved from https://honeytarg.cert.br/honeypots/stats/flows/current/
10 Retrieved from https://cert.br/stats/honeypots/
11 Retrieved from https://www.shadowserver.org
12 Retrieved from https://www.shodan.io

PROFILE OF SECURITY INCIDENTS REPORTED TO CERT.br

Since 1999, CERT.br has maintained official statistics on incidents reported voluntarily to the team. As shown in Chart 1, the number of such reports has presented a rising tendency over the years. There are multiple factors that have led to this increase, among which is the growth of the Internet. As more and more devices are connected to the Internet, exposed vulnerabilities increase, as does the interest of attackers.

In 2014, as illustrated in Chart 1, there was a sudden spike in the number of reports. From then onwards, the numbers rose to a new threshold, always above 600 thousand per year. Moreover, the attack categories with the highest number of reports that year are the same ones reported in the following years, which is why a more detailed analysis on such attacks is presented below. The analysis specifies the attacks, the breakdown in 2014, and how this situation has evolved until 2019.

CHART 1 - TOTAL NUMBER OF INCIDENTS REPORTED TO CERT.br PER YEAR



SOURCE: CERT.br

The high number of incidents in 2014 was due to three categories of attacks: fraud attempts, scanning and denial of service attacks.[13][14] That year, 467,621 fraud attempts were reported, five times higher than in 2013, and accounted for 44% of all the reports received by CERT.br in 2014. Cases of fake bank webpages and e-commerce websites (classical phishing) increased by 80%, and cases of fake webpages not related to financial fraud, such as webmail services and social networks, increased by 73% in that year. It is important to point out that the prime objective of such attacks is to capture access credentials used to log in to websites, corporate systems, and e-mail accounts, among others.

Scanning attacks are aimed at identifying which computers are active and which services are being made available by these computers. In 2014, reports on such attacks totaled 263,659, a 59% increase. Services vulnerable to brute-force attacks, that is, attacks whose objective is to repeatedly test accounts and passwords until access credentials are guessed, were the services with the highest number of searches: SSH (22/TCP) accounted for 21% of the scanning reported in 2014, FTP (21/TCP) accounted for 12% and TELNET (23/TCP) accounted for 10%.

Regarding denial of service (DoS) attacks in 2014, a total of 223,935 reports were received related to IPs allocated to Brazil that participated in DoS attacks, which is 217 times higher than the number of reports received in 2013 for the same category. Most reports were related to improperly configured devices located in Brazil, and which were overwhelmingly targeted to expand the denial of service attacks. In other words, these devices contained enabled services that exposed network protocols on the Internet that could be used for amplification,[15] such as: CHARGEN (19/UDP), DNS (53/UDP), NTP (123/UDP), SNMP (161/UDP) and SSDP (1900/UDP). Together, these five protocols corresponded to more than 90% of DoS reports in 2014. The remaining 10% of reports were related to devices infected by bots. Bots are malicious

13 Retrieved from https://cert.br/stats/incidentes/2014-jan-dec/analise.html

14 Retrieved from https://www.nic.br/noticia/releases/cert-br-registra-aumento-de-ataques-de-negacao-de-servico-em-2014/

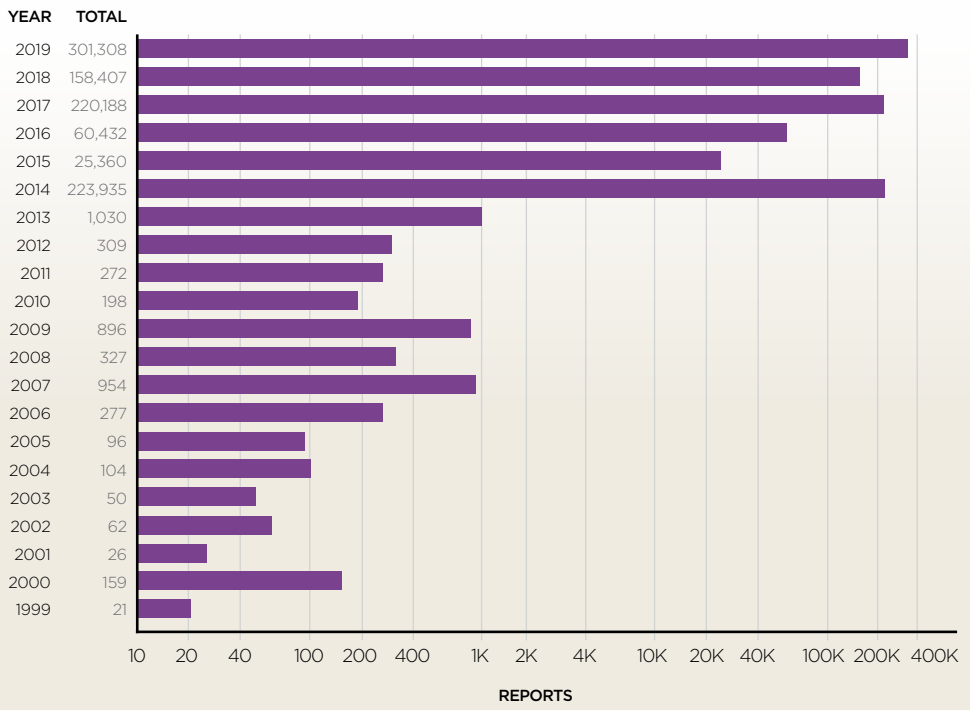
15 Alert (TA14-017A) UDP-Based Amplification Attacks, Cybersecurity and Infrastructure Security Agency (CISA). Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-017A

codes with mechanisms that communicate with the attacker and allow them to be remotely controlled so that attacks such as denial of service are triggered against third parties. Networks with hundreds or thousands of bots controlled by a attacker are called botnets.

These three types of attacks altogether corresponded to 91.23% of all the attacks reported in 2014. Scanning and attempts at fraud were two categories that used to correspond to a significant part of the reports, but the DoS attack category has grown significantly since then, as illustrated in Chart 2. In the years prior to 2014, the DoS category accounted for less than 1% of the reports. Since 2014, it has accounted for a significantly higher number of reports

CHART 2 – REPORTS ON DEVICES: PARTICIPATING IN DoS ATTACKS

Logarithmic scale



SOURCE: CERT.br

In the period from 2015 to 2018, most denial of service attacks reported to CERT.br were related to devices generating amplifications. However, one situation had already been drawing attention; namely, the year-to-year increase of reports on DoS attacks originating from botnets. Such attacks came from infected devices that could be broadly characterized as Internet of Things devices, such as security cameras, Digital Video Recorders/DVR), smart TVs, hard disk drives, WiFi and broadband routers.

In 2019, CERT.br received 875,327 reports of security incidents. Of these, 301,308 were reports on devices that were involved in denial of service attacks, which was a record high. Most of the referred reports were on UDP flood attacks generated by IoT botnets such as Mirai and Bashlite, which infect devices such as DVRs and broadband routers. Those types of attacks had already been reported since 2015, but they grew significantly in 2019.

This change in attack patterns, from amplifications to IoT botnets, is probably related to two concurrent factors: the drop in the number of amplifications and the increase in the number of IoT devices connected to the Internet. These factors will be addressed in more detail in the next sections which will focus on data from honeypots and external sources.

In relation to statistics on the most frequent incidents reported in 2019, it is important to point out that most scan notifications were for services that enable brute-force password attacks.

According to scanned TCP ports, such attacks are divided into the following categories:

- Brute-force attacks on network servers' access credentials, on routers, and on IoT devices (ports 22, 23 and joint search through ports 23 and 2323);
- Brute-force attacks on e-mail passwords (ports 25 and 143);
- Brute-force attacks on access credentials and vulnerabilities of Winbox MikroTik (joint search through ports 23 and 8291).

A comparison of the most frequently attacked ports in 2014 with the ones in 2019 shows that the number of ports has increased. In addition, attacks on e-mail services also increased. This focus by attackers on access credentials is also corroborated by several external studies conducted by secu-

rity companies that keep track of the underground market. The analysis on page 5 of TrendMicro's 2020 report, the title of which is "Shifts in Underground Markets Past, Present, and Future,"[16] mentions that access credentials and stolen accounts are the majority of the "goods" being offered in the underground market. Access credentials to bank accounts, e-mail accounts, social media accounts, entertainment services, among others, are the most common targets. This study also included IoT vulnerabilities, botnets, and denial of service attacks among such "goods." This evidences that the most frequent incidents reported to CERT.br are consistent with the goods and services most actively traded by the attackers.

MOST FREQUENT ATTACKS ON DISTRIBUTED HONEYPOTS MAINTAINED BY CERT.br

As mentioned above, CERT.br maintains a distributed honeypots network. These are 100% passive sensors and which, in an ideal Internet where attacks would never occur, would not receive any traffic, because no service is provided by these sensors. This type of sensor allows the Internet's background noise to be detected; that is, the constant traffic generated by malicious codes attempting to spread throughout the networks and the noise generated by attackers scanning IPv4 addresses in search of vulnerable or poorly configured systems. Below is an analysis of all the attacks on these sensors in 2019[17] and the comparison with 2018.[18] In addition, the analysis sheds light on how this data complements the data on incidents reported to CERT.br. In relation to the scanning of TCP ports, the following attacks were the most significant:

- Scanning through ports TCP 23, 22, 81, 5555, 8000, and 8080 are related to activities to spread IoT botnets, such as Mirai and its variants, and Bashlite and its variants. Attacks on these ports are brute-force attempts on access credentials or attempts to exploit vulnerabilities of broadband or WiFi router management interfaces.

16 Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf
17 Retrieved from https://cert.br/stats/honeypots/
18 Retrieved from https://cert.br/stats/honeypots/2018/

- There was an increase in scanning of e-mail services, mostly through ports POP3 (110/TCP), SMTPS (465/TCP), IMAPS (993/TCP), and POPS (995/TCP). This increase could be related to the increase of brute-force attacks on other e-mail services, as informed in the security incidents reported to CERT.br.
- From 2018 to 2019, the number of packets against the RDP (Remote Desktop Protocol) increased by 546%. This growth coincided with the announcement of a vulnerability called BlueKeep (CVE-2019-0708[19]), which started being exploited by several malicious codes.

In relation to traffic directed at UDP ports, below are the points to be highlighted:

- The UDP port with the highest number of scanning attacks continues to be the 5060/UDP, which increased by 32% from 2018 to 2019. This activity is related to the abuse of SIP servers, through brute-force attacks on access credentials for extensions used for long-distance calls.
- Another point worth mentioning is the continuity of scanning attacks targeting services vulnerable to abuse through traffic amplifications. The servers are: SNMP (161/ UDP), NTP (123/UDP), DNS (53/UDP), SSDP (1900/UDP), Netbios (137/UDP), Chargen (19/UDP), Portmap (111/ UDP), mDNS (5353/UDP), TFTP (69/UDP), and qotd (17/ UDP). These scanning attacks are probably carried out by attackers attempting to map amplifications to then abuse them by means of denial of service attacks.

It is interesting to note that, among the malicious activities most frequently observed by honeypots, are various scanning attacks related to the spread of IoT botnets, as well as the search for amplifications and the mapping of services vulnerable to brute-force attacks on access credentials. All these activities are also among the most frequent attacks mentioned in the incidents reported to CERT.br.

19 Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

THE PROBLEM OF AMPLIFICATIONS THAT ALLOW DENIAL OF SERVICE ABUSE

As pointed out in the analysis of incidents reported to CERT.br, the year 2014 was highlighted by the increase in the number of DoS attacks with the use of amplifications of badly configured UDP protocols exposed on the Internet. For a better understanding of the impact of these attacks and the difficulties of reducing them, below is a description of the evolution of such attacks since the middle of the 2000s.

The first amplification attacks occurred in 2007, and specifically targeted the DNS protocol. These were cases in which recursive servers were badly configured and would answer questions that came from any point on the Internet. This attack was so effective that it was used to take down root name DNS servers. At that time, CERT.br had already written a document[20] explaining the problem and how to remedy it. CERT.br had also initiated a process to notify Brazilian networks allowing DNS amplification to correct this.

Amplification attacks basically abused the DNS protocol. In 2013, researcher Christian Rossow wrote a paper on protocols that allow amplification, published at the NDSS Conference. At that time, Rossow worked together with the US-CERT to develop the TA14-017A Alert,[21] launched in January 2014. This brought up the issue again for the technical community, and another 11 UDP protocols allowing amplification were described. The alert and the article put this issue into the spotlight, which resulted in the development of new denial of service attack tools, the use of which became widespread in 2014. This in turn led to the increase in the number of incidents reported to CERT.br, and to the growth in the number of denial of service attacks.

In March 2014, as a reaction to this new scenario, the Shadowserver Foundation initiated a project with the objective of scanning the entire IPv4 address space in search of

---

20 Recommendations to Avoid the Abuse of Open Recursive DNS Servers (*Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos*); Cristine Hoepers, Klaus Steding-Jenssen, Nelson Murilo, Rafael R. Obelheiro. Retrieved from https://cert.br/docs/whitepapers/dns-recursivo-aberto/

21 Alert (TA14-017A) UDP-Based Amplification Attacks; Original release date: January 17, 2014; Last revised: December 18, 2019. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-017A

the services listed in the US-CERT's alert and that allowed amplification.[22] This became an on-going project, which has been constantly updated to add more protocols for testing. The project generates two types of data: official statistics of countries with the most amplification attacks and data broken down per country IPs allocation. This data is shared with the national CERTs of those countries. Shadowserver data is also shared with CyberGreen,[23] which maintains official statistics on the data, including a panel that shows the potential of global denial of service attacks and a list of countries with the highest number of devices allowing amplification.[24][25]

In 2015, CERT.br started to compile Shadowserver data related to DNS and NTP amplifications in IPs allocated to Brazil and forwarded periodic reports in this respect to the parties responsible for the Autonomous Systems of those IPs. The reports included detailed instructions on how to solve the problem. However, as the years went by, the number of devices allowing amplification started to change the profile of the server networks due to badly configured services. This led to a scenario in which many of those devices allowing amplification were broadband routers and network devices. These are devices that do not need and do not use most of the services that allow amplification, as they come from the manufacturers with open services, on account of faulty development policies, poor software integration and standard configuration. The bad practices of home router manufacturers were extensively described in the publication "Home Router Security Report 2020," which addressed several serious problems, especially the use of old-fashioned and outdated operating systems by these manufacturers.

In the period from 2014 to 2017, several organizations published manifestoes for the adoption of best network practices, mainly to avoid spoofing (falsification of the origin IP address

22 The scannings will continue until the Internet improves. Retrieved from https://www.shadowserver.org/news/the-scanningnings-will-continue-until-the-internet-improves/

23 The CyberGreen Institute is a collaborative, non-profit organization that develops activities for a healthier and more resilient Internet. Retrieved from https://www.cybergreen.net/who-we-are/

24 CyberGreen Country Overview. Retrieved from https://stats.cybergreen.net/country

25 In 2017, when CyberGreen started to divulge statistics, Brazil was the number 1 country in terms of service denial "firepower."

of a TCP/IP packet). This is a problem caused by the bad configuration of networks and is the prime situation that allows an attacker to start an amplification attack.[26] One of the first manifestoes of this kind was the "Routing Resilience Manifesto – Draft 1," which was put up for discussion by the Internet Society (ISOC) between June and July 2014. This manifesto was officially published on August 31, 2014, under the title "Mutually Agreed Norms for Routing Security (MANRS)."[27] The document does not focus mainly on reducing amplification, and one of its four pillars is the implementation of anti-spoofing measures.

The Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG) was another group that was actively discussing this issue at that time. The LAC-AAWG group is part of LACNOG, a regional forum of network operators assisted by the Internet Addresses Registry for Latin America and the Caribbean (LACNIC). LACNOG, comprised of regional network operators, was discussing the impact of broadband routers' vulnerabilities on the resilience of Internet Service Providers (ISPs). At a meeting held in October 2017, the forum decided to prepare a document containing a set of minimum-security requirements that should be taken into account when CPEs[28] (Consumer Premises Equipment) are acquired by Internet Service Providers (ISPs). This best practice was developed jointly by LAC-AAWG and M3AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group). It was revised by a panel of external experts and published on May 6, 2019.

The main point of this best practice is that the CPEs must leave the factory with more robust configurations. They must allow firmware updates and should not be delivered equipped with unnecessary services, such as those allowing amplification, turned on by default. This was a consensus, and the problems were pointed out as being the reason for the high number of infected broadband routers allowing amplification.

---

26 Antispoofing. Retrieved from https://bcp.nic.br/antispoofing

27 MANRS History. Retrieved from https://www.manrs.org/about/history/

28 CPE (Customer Premise Equipment) is the equipment used to connect subscribers to the network of an Internet Service Provider (ISP). Examples of CPE include modems (cable, xDSL, fiber) and home WiFi routers, among others.

In view of this scenario, at the end of 2017, the Brazilian Internet Steering Committee (CGI.br) and the Brazilian Network Information Center (NIC.br) launched at the IX Forum 11 a program called "For a safer Internet" (*Programa i+seg*). The Program was developed with the support of SindiTelebrasil, the Brazilian trade association of telecom operators, and of ABRANET and ABRINT, the Brazilian trade associations of Internet access providers, and in partnership with the Internet Society.[29] The objective of the Program is to provide support to the Internet technical community to reduce the number of denial of service (DDoS) attacks originating from networks in Brazil, reduce prefix hijacking and route leaks, prevent the faking of source IP addresses, decrease vulnerabilities and configuration flaws existing in network elements, and bring together the teams responsible for network security and stability. The program's ultimate objective is to develop a culture of security among network operators. These best practices are basically MANRS, the hardening of devices and the reduction of amplification mechanisms.

The metrics on the amplification situation in Brazil are drawn from work done by CERT.br using the data received from Shadowserver and Shodan.[30] Based on this data, CERT.br identifies all the IP addresses pointed out as allowing amplification. At this point, CERT.br runs its own tests for each amplification category, and stores information on the test's timestamp and on result details. This data is grouped by ASN, and a report with details on the test and instructions on how to solve the problem are sent to each party responsible for the Autonomous Systems. From July 2018 to December 2019, the number of IPs allocated to Brazil allowing amplification and present in Shadowserver and Shodan data dropped by approximately 60%, especially in the SNMP[31] category. This decrease is linked to CERT.br notifications and to meetings with Internet providers and service operators, part of *Programa i+seg*, which has contributed significantly to raise awareness of Internet

29 Retrieved from https://bcp.nic.br/i+seg/sobre/

30 Statistics on reported IPs and ASNs Allowing Amplification. Retrieved from https://cert.br/stats/amplificadores/

31 Retrieved from https://www.nic.br/noticia/releases/estatisticas-do-cert-br-apontam-aumento-de-ataques-de-negacao-de-servico-em-2019/

operators and providers in regard to network infrastructure best practices. As mentioned previously, this measure also lowered the number of reports on DoS attacks involving amplification mechanisms sent to CERT.br. In addition, it improved Brazil's position in the CyberGreen ranking. Brazil now ranks as the eighth country on this list with the most "firepower," a ranking which is compatible with the size of our network in terms of domains and number of allocated IP addresses, in comparison to other countries.

HOW TO ACHIEVE THE PARETO PRINCIPLE TO REDUCE INCIDENTS

In the introduction to this article, as a provocation, three security measures were mentioned which could reduce the number of security incidents reported to CERT.br by at least 80%. The next step was to address the most frequent attacks, their prevalence, and causes. Below are the three afore-mentioned measures, pointing out how each of the problems referred to above can be solved through such measures:

1. **Keep all software (operating systems and applications) updated.** As mentioned above, most attacks use botnets and depend on infecting devices. This means compromising a device in some way, either by getting the access credentials right (topic of item 3 below) or exploiting vulnerabilities. US-CERT posted some unsettling – but not surprising – statistics, which stated that the 10 most common vulnerabilities exploited to compromise government network systems are all well known, and remedies are available, some of which have been available for more than 5 years.[32] The same situation holds true for vulnerabilities exploited by botnets such as Mirai and Bashlite, referred to in this article.
2. **Harden all systems and devices.** As previously mentioned, even systems that have been updated will be abused by different attacks if their original configurations, standard passwords, and other original features remain in place. Amplification attacks occur basically

32 Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities; May 12, 2020. Retrieved from https://us-cert.cisa.gov/ncas/alerts/aa20-133af

because no systems hardening was implemented, especially in home routers and network devices. However, this problem also occurs with services that are exposed on the Internet.

3. **Improve identification and authentication processes for logging in to services and systems**. Attackers will always choose the easiest way in. Nowadays, systems that only use passwords are the norm, and this is the way that leads to most of the attacks, to the compromising of IoT, among other problems. Many systems do not have multi-factor authentication. Raising awareness in this respect requires educating users extensively on how to choose and manage adequate passwords and how to protect their access credentials.

These three measures, which seem simple, are essential to achieve a healthy ecosystem. Many people refer to this as digital hygiene, but implementing the three measures does not depend upon one sole player in the chain. This depends on the entire chain of suppliers, IT and security professionals, and users.

These actions will not solve all problems; however, if everybody implements those measures, the result will be a drop in the number of incidents to more manageable thresholds, and will allow organizations to focus on managing the other 20% of risks, without having to worry about the 80% of attacks that occur for known reasons and for which well-established solutions are available.

SOME THOUGHTS ON HOW TO ACHIEVE A HEALTHY ECOSYSTEM

As mentioned, achieving a healthy ecosystem, and reducing risks depends on several factors. It depends on the software being used, on the training of the professionals and on the efforts of each and every one of us to do our share. For example, in the case of denial of service attacks it is necessary to weaken the "firepower" of the attackers. However, it is not the attacked networks that should do this; rather it is the networks that in principle are not being affected by this problem.[33] This is a classic case of

33 Recommendations to Improve the Scenario of Distributed Denial of Service (DDoS) Attacks (*Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)*); CERT.br. Retrieved from https://cert.br/docs/whitepapers/ddos/

lack of incentives for implementation, and it is necessary for all networks connected to the Internet to implement measures that will benefit everybody but will not necessarily bring immediate benefits to those who implement the actions. Below are some thoughts on crucial processes that should be implemented in all organizations and that could make a huge difference in terms of reducing security incidents on a large scale.

- **Everything begins with the right choice**. When choosing a software or hardware supplier (including for items such as cameras, printers, lights, nametag control systems or any other "smart" item), it is necessary to get acquainted with their updating policies (also known as patches, fixes, and updates). In other words, the product has to offer a constant, online updating program and must make it clear how to contact the manufacturer to report problems and get information on updates.
- **Do not rely only on passwords to protect access**. Set up multi-factor authentication (MFA, also referred to as 2FA) in the equipment and choose online services that allow you to use MFA/2FA. As mentioned previously, most of the attacks reported to the CERT.br in the last 5 years included password cracking and password guessing. The attacks also included, among others, access passwords to: cloud services, back-ends of virtual stores, e-mail accounts, local servers at companies, desktops, devices such as cameras and external hard drives, access credentials to online services, and social media accounts.
- **Always fix the problem; do not postpone correcting it.** It is essential that all operating systems, services, and applications used by companies always run on the latest version, with all the proper security mechanisms in place. This prevents the company from being compromised by malicious codes that exploit vulnerabilities in these systems. And above all, do not forget to consider "things": cameras, printers, broadband modems, WiFi routers, lamps, smart TVs, among other connected devices. They can also be infected and launch attacks.

- **Conduct periodic checks by qualified security professionals.** Big corporations are able to set up more robust protection mechanisms by maintaining teams dedicated to risk management, security and treatment of incidents. Small and medium-sized businesses operate in a different scenario, where there are no professionals dedicated to information and communication technology (ICT). It is crucial that these companies find some way to periodically revise their configurations, review security measures and implement improvements, either by their own personnel or by third parties.
- **Educate employees.** At most companies that were invaded, or that underwent data leaks, the starting point was phishing, which is a fraudulent message, targeted at a company employee. Phishing can be in the form of an e-mail impersonating the boss, an "urgent" message from another messaging service, or even a visit to a legitimate, yet infected website. From the starting point, the invasion permeates the entire network, and the result can be a data leak, data hijacking for ransomware, financial frauds or even the use of the company's network to commit crimes and attack third parties. It is necessary to educate people so that they also follow basic hygiene measures: always run the systems' latest version, immediately apply all security fixes, avoid accessing unfamiliar links, do not believe in business propositions that sound too good to be true, and use basic security tools.

The three measures discussed in this article are simple because they do not require special tools or the development of new technologies. Their implementation depends on the implementation of processes, investments in human resources – these are steps that must be prioritized by managers and that require the understanding that there is no ready-made tool or solution to solve the problem.

REFERENCES

Ceron, J. M., Steding-Jessen, K., & Hoepers, C. (2012). Anatomy of SIP Attacks. *Usenix; login magazine, 37*(6), 25-32. Retrieved from https://www.usenix.org/publications/login/december-2012-volume-37-number-6/anatomy-sip-attacks

Ceron, J. M., Steding-Jessen, K., Hoepers, C., Granville, L., & Margi, C. (2019). Improving IoT Botnet Investigation Using an Adaptive Network Layer. *Sensors, 19*(3), 727. Retrieved from https://doi.org/10.3390/s19030727

CGI.br (2012). Mecanismos de Segurança. In *Cartilha de Segurança para Internet* (Chapter 7, pp. 47-58). São Paulo: CGI.br. Retrieved from https://cartilha.cert.br/livro/

CGI.br (2020). Cuidado com o que sai da sua rede. *Revista.br* (17ª ed.). Retrieved from https://cgi.br/publicacao/revista-br-ano-11-2020-edicao-17/

Desiderá, L., Steding-Jessen C., & Hoepers, C. (2019). Requisitos Mínimos de Segurança para CPEs: a Experiência de Construir uma Recomendação Global. *V Workshop on Regulation, Conformity Evaluation, Tests and Security Patterns* (WRAC+), São Paulo, SP. Retrieved from https://cert.br/docs/papers/bcop-cpe-wrac2019.pdf

ENISA (2011). *Proactive detection of network security incidents, report*. Retrieved from https://www.enisa.europa.eu/publications/proactive-detection-report

FIRST (2019). *FIRST Computer Security Incident Response Team (CSIRT) Services Framework*, Version 2.1. Retrieved from https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

FKIE (2020). *Home Router Security Report 2020*. Retrieved from https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

Hoepers, C., Steding-Jessen, K., Cordeiro, L. E. R., Chaves, M. H. P. C. (2005). A National Early Warning Capability Based on a Network of Distributed Honeypots. *17th Annual FIRST Conference on Computer Security Incident Handling*, Singapore, SG. Retrieved from https://cert.br/docs/papers/early-warning-first2005.pdf

Internet Governance Forum (IGF). (2014). *Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security*. Retrieved from https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file

Marzano, A., Alexander, D., Fazzion, E., Fonseca, O., Cunha, Í., Hoepers, C., . . . Meira Jr, W. (2018). Monitoramento e Caracterização de Botnets Bashlite em Dispositivos IoT. *XXXVI Brazilian Symposium on Computer Networks and Distributed Systems*, Campos do Jordão, SP. Retrieved from https://honeytarg.cert.br/honeypots/docs/papers/honeypots-sbrc18.pdf

Marzano, A., Alexander, D., Fonseca, O., Fazzion, E., Hoepers, C., Steding-Jessen, K., . . . Meira Jr, W. (2018). The Evolution of Bashlite and Mirai IoT Botnets. *IEEE Symposium on Computers and Communications*, Natal, RN. Retrieved from https://honeytarg.cert.br/honeypots/docs/papers/honeypots-iscc18.pdf

Rossow, C. (2013). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. *NDSS Symposium 2014*, San Diego, CA. Retrieved from https://www.ndss-symposium.org/ndss2014/programme/amplification-hell-revisiting-network-protocols-ddos-abuse/

CHAPTER 4

Digital security and risk management: An analysis of Brazilian enterprises[1]

Stefania L. Cantoni,[2] Leonardo M. Lins,[3] and Tatiana Jereissati[4]

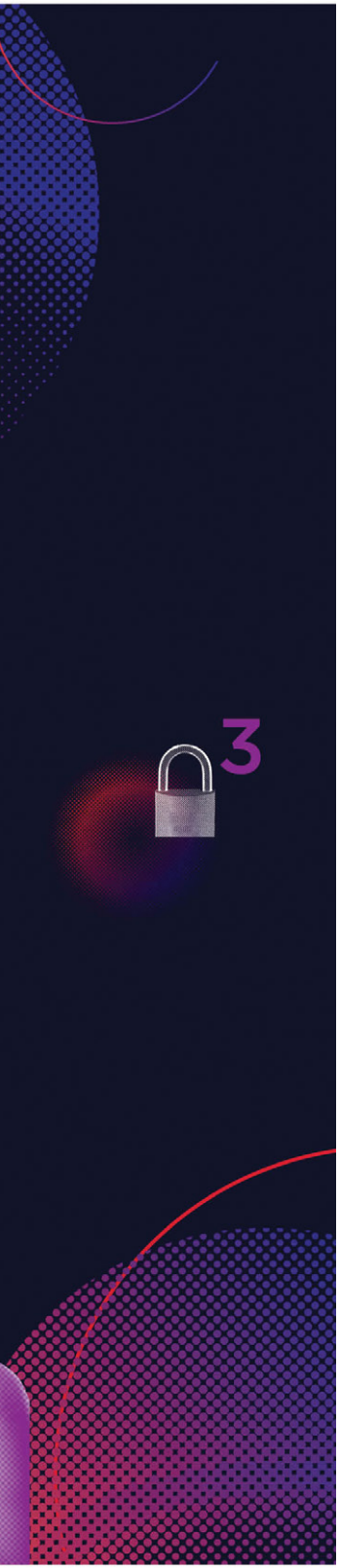
1 We would like to thank Fabio Senne (Cetic.br|NIC.br) for his attentive reading and suggestions for this chapter.

2 She holds a master's degree in Political Science from the University of São Paulo (USP) and is a researcher at the Qualitative Methods and Sectoral Studies Coordination at Cetic.br|NIC.br.

3 He holds a PhD and a master's degree in Sociology from USP and is a researcher at the Survey Project Coordination at Cetic.br|NIC.br, where he coordinates the ICT Enterprises and ICT Providers surveys.

4 She holds a postgraduate degree in Social Sciences with special mention to Gender and Public Policies from Facultad Latinoamericana de Ciencias Sociales (FLACSO-Argentina) and is the coordinator of Sectoral Studies and Qualitative Methods at Cetic.br|NIC.br.


2
1



INTRODUCTION

In the last decade, information and communication technologies (ICT) have been consolidated as an important vector for development in different sectors of society in a context where the digital environment becomes increasingly significant for the activities of governments, enterprises, and individuals (OECD, 2015), and the data-driven economy becomes more and more relevant.

Given the importance of ICT to drive the competitiveness of countries, much has been debated about the advances of the digital economy and the positive and negative effects of the broad digitalization of production processes. On the one hand, there is an intense debate about the benefits of technological advances in the digital age and the consequent efficiency gains of a highly connected economy, which poses a new production paradigm that has effects in several sectors (Schwab, 2016; Brynjolfsson & McAfee, 2014). On the other hand, there are more cautious views on the advance of the digital economy, especially when it comes to changes in labor relations, increased income concentration, job destruction, as well as new threats that arise from taking advantage of the vulnerabilities created by the intensified interconnection of individuals and organizations (Srnicek, 2016; Frey & Osborne, 2017). In this new context, different sectors are challenged to adapt so that they are able to reduce disadvantages and increase the gains arising from a highly connected economy (OECD, 2017; UNCTAD, 2019). However, the different organizations that make up the economic scenario have unequal capacities to adapt to the context of digital transformation; if these gaps are not addressed, regional and economic inequalities could become deeper (OECD, 2015).

In the current context of transformation driven by advances in Artificial Intelligence (AI), analysis of Big Data and cloud computing, added to the increase in the total number of individuals and devices connected to the Internet, it becomes especially important to discuss the consequences arising from the growing digitalization of enterprises in Brazil and its implications for the management of these organizations. Given that the productive sector is one of the most affected by the

ongoing digital transformation, understanding how different enterprises have been dealing with the adjustment of their routines to new technologies will allow the portrayal of an overview of the effects of a more connected economy. Among the topics related to digitalization and the adjustment of business processes, special mention should be made to digital security incidents and their effects, which result from a growing exposure to the digital environment and an increasing dependence on the interconnection of digitalized processes and presence in networks. Thus, this chapter aims to discuss how a group of Brazilian enterprises conduct their digital security risk management. From a qualitative approach, we seek to analyze the view that small, medium and large Brazilian enterprises from different segments of economic activity have on digital security risks, as well as to find out if they have processes to manage these risks and how they implement them, including the assessment of potential consequences, how they handle them, and the limitations faced by these enterprises to develop mature digital security risk management.

ORGANIZATIONS, UNCERTAINTIES AND RISK MANAGEMENT

Generally, in decision-making processes, risk relates to the amount and quality of existing information about a given situation; thus, it is understood that risks will vary according to the uncertainty about the likelihood of an event occurring (March, 1994). Although organizations tend to avoid uncertainty – and mobilize, as their main resources, the creation of standards for collecting and processing information and establishing internal routines –, several factors can undermine these forms of anticipating and controlling events, leading to adverse situations (March, 2010).

Risk management is, therefore, the act of mitigating unanticipated results arising from the variation of information about the environment in which enterprises operate (March & Shapira, 1987; OECD, 2015). Risks are not only the result of scarcity of information, but also of individual cognitive limitations that restrict the ability to process and interpret information as a whole, which increases the chances of courses of action going out of line and generating unexpected events (March, 1994).

Allied to this, the interconnection of processes between diverse organizations means that they are not isolated from problems that may occur with others, generating unforeseen reactions in chains that require immediate actions, which are not always included in the repertoire of routines (Perrow, 1999).

Although risks cannot be completely avoided, it is important that organizations make efforts to manage them properly. Taking risks is at the base of an enterprise's activity: the development of a new product, a change in the business model or the search for new markets are actions shrouded in uncertainties that, if avoided at all costs, constrain the organization's capacity to explore new things that can bring them positive returns. Thus, it is important for enterprises to direct resources towards the constant creation and accumulation of knowledge about the environments in which they operate, in order to reduce uncertainties and mitigate risks, seeking to expand and improve their scope of action and performance (Pisano, 2017).

DIGITAL SECURITY RISK MANAGEMENT

Organizations are also exposed to risks resulting from the adoption of ICT and the interconnection of networked systems and devices. Due to its dynamic nature, risks related to digital security can originate from threats and vulnerabilities arising from the digital environment, and affect the achievement of economic and social objectives, as it undermines the "CIA triad," that is, confidentiality, integrity, and availability of activities.

It is important to note, however, that digital risk is not only related to uncertainty regarding the use of the digital environment. The reliance on the digital environment requires not only software and hardware, but also human intervention – either directly or indirectly. All of these aspects are subject to threats, vulnerabilities and incidents.

The effects of these uncertainties on tangible and intangible assets of organizations have an economic and social nature, thus the risk of digital security must be formulated in economic and social terms, not purely in technical terms (OECD, 2015).

In this context, Digital Security Risk Management (DSRM) becomes relevant, which is defined by the Organisation for Economic Co-operation and Development (OECD) as the "the set of coordinated actions taken within an organisation and/

or among organisations, to address digital security risk while maximizing opportunities" (OECD, 2015, p. 8). DSRM comprises decision-making and a general framework for managing inherent risks in economic and social activities, guided by a holistic, systematic and flexible set of cyclical processes which help ensure that DSRM measures are "appropriate to and commensurate with the risk and economic and social objectives at stake" (OECD, 2015, p. 8).

Four possible strategies for organizations to handle digital risk are presented below.

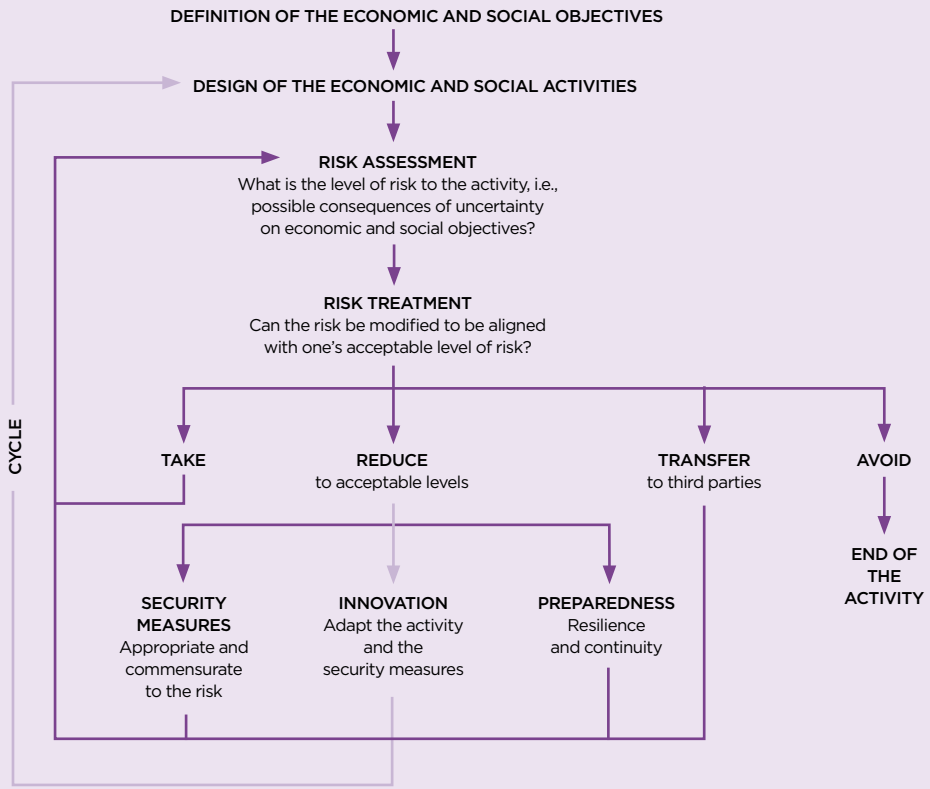
DIGITAL SECURITY RISK MANAGEMENT: FOUR STRATEGIES

- **Accepting the risk:** "taking the risk" and accepting the effect of uncertainty on the objectives, including partial or complete failure. If the activity is undertaken, risk cannot be entirely eliminated, therefore, some "residual" risk must be accepted. In general, risk management is economically efficient when the benefits gained from carrying out the activity outweigh the residual risk.
- **Reducing the risk:** to reduce it to the acceptable level *(i)* selecting and applying security measures to protect the activities against certain potential threats exploiting vulnerabilities identified in the risk assessment; *(ii)* changing the activity, for example by redesigning or operating it differently, which can lead to innovation; and *(iii)* defining and, as necessary, operating preparedness measures to cope with the occurrence of incidents.
- **Transferring the risk:** moving the unwanted effects of uncertainty on the activity's objectives to someone else, for example by contract such as through insurance.
- **Avoiding the risk:** eliminating it by not carrying out the activity or eliminating its digital element.

SOURCE: ADAPTED FROM OECD (2015).

Because risks are inherent to the operations of organizations, the OECD also highlights the importance of the risk management cycle for the activities of enterprises, especially as an input for decision-making processes (OECD, 2015). Figure 1 represents the risk management cycle based on the operational principles of the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity.

FIGURE 1 – OVERVIEW OF THE RISK MANAGEMENT CYCLE BY ORGANIZATIONS



SOURCE: OECD (2015).

According to the flow proposed by the model, one should start with the definitions, objectives, and design of the organizational activity. Then, specific risks can be assessed and addressed according to the approach deemed as the most appropriate, so that the initial objectives are preserved and supported (OECD, 2015). To better understand how the risk management process takes place in organizations, it is paramount to develop indicators that portray this reality.

DIGITAL RISK MEASUREMENT IN ENTERPRISES

According to the United Nations Conference on Trade and Development (UNCTAD), only 4% of developing countries produce data on the use of ICT in enterprises, while this percentage is 85% among developed countries (UNCTAD, 2019). This gap means that less developed countries also have less information to formulate policies that promote the development of the digital economy.

The capacities and resources of countries to measure such phenomena have not kept up with the accelerated pace of digital transformation. In addition to the lack of human and financial resources for this task, there are a series of methodological challenges that contribute to this scenario of low data production, which is aggravated in the context of digital security. The reasons for this include the lack of standardized definitions of concepts, typology, and taxonomy, which makes the process of producing comparable data difficult. Added to this is the historical scarcity of data on topics linked specifically to digital vulnerabilities, threats, and incidents (OECD, 2019b). The absence of a methodological standard to guide the production of data is a challenge for the development of public policies that address this issue (OECD, 2019b).

In order to bridge this information gap and contribute to the creation of data repositories on this topic, after the 2016 Cancun Ministerial Meeting on the Digital Economy,[5] the OECD started a project to map surveys with data on digital security risk. The analysis of existing surveys revealed that only a small number included questions about digital security risk management practices; when such questions where present, the indicators were restricted to technical measures (OECD, 2019b). In this scenario, the OECD created the Measuring Digital Security Risk Management Practices in Businesses initiative, as detailed below.

5 The Ministerial Declaration on the Digital Economy, or "Cancún Declaration" is available at: https://www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf

THE OECD INITIATIVE: MEASURING DIGITAL SECURITY RISK MANAGEMENT PRACTICES IN BUSINESSES

In an effort to provide parameters for enterprises to assess their own DSRM practices, as well as to inform public policies aimed at increasing the maturity level of enterprises with regard to DSRM, the OECD (2019a) developed the project "Measuring Digital Security Risk Management Practices in Businesses," that aimed at promoting the measurement of DSRM practices, mainly in small and medium-sized enterprises (SME) in different economic sectors. According to the OECD (2017), SME comprise most of the business population and contribute greatly to job and value creation; also, there is a dearth of relevant, reliable, and rigorous evidence on DSRM practices in SME.

In line with the principles of the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity, the organization has developed a framework for measuring digital security risk management practices in businesses (see p. 132). Structured in three phases,[6] conducted between February 2017 and November 2018, the project was part of the Going Digital project, which aims at providing, especially for policymakers, the tools needed to help the economy and society thrive in an increasingly digital and data-driven world.[7]

6 The OECD report on the three phases of the project can be accessed at: https://www.oecd-ilibrary.org/science-and-technology/measuring-digital-security-risk-management-practices-in-businesses_7b93c1f1-en

7 The OECD's Going Digital project is currently in its second phase, from 2019 to 2020, marked by the launch of the Going Digital Toolkit (https://goingdigital.oecd.org/en/). The first phase, from 2017 to 2018, was concluded with the Going Digital Summit and the launch of "Going Digital: Shaping Policies, Improving Lives" and "Measuring the Digital Transformation: A Roadmap for the Future." More information at: http://www.oecd.org/going-digital/project/

MODULES FOR MEASURING RISK MANAGEMENT PRACTICES ACCORDING TO THE OECD FRAMEWORK

By adopting a modular structure, the framework proposed by the OECD allows the measurement of key concepts[8] in a comparable way at the international level, in addition to enabling countries to adapt it to the specific needs of each national context. The six dimensions covered by the framework are detailed below:

- **Module A –** Demographic information on the enterprise: size, sector of activity, and annual revenues. It measures the enterprise's digital intensity based on the combination of selected indicators on ICT use.
- **Module B –** Digital security risk governance: it assesses whether there is an appropriate DSRM governance framework in the respondent enterprise.
- **Module C –** Digital security risk assessment practices: it maps the three-step risk assessment process (identification, analysis, and evaluation of information); it seeks to determine whether the risk assessment process takes into account the consequences of uncertainty for other stakeholders; and the outcome of the risk assessment process.
- **Module D –** Digital security risk reduction practices: it measures which risk reduction practices were selected and operated and what risks these practices were intended to reduce, and understands the reason for the risk reduction decisions (that is, if they were the consequence of a risk assessment process).
- **Module E –** Digital security risk transfer practices: it measures actions or processes used to transfer the unwanted effects of uncertainty to other parties in business activities. It focuses on the use of insurance (e.g., policies and their respective coverage), measures what risks are transferred, and understands the reason for the risk transfer decisions (i.e., whether they were the consequence of a risk assessment process).
- **Module F –** Digital security risk management awareness and training: it measures the respondent's awareness of the effects that digital security risk can have on the achievement of an enterprise's economic and social objectives, and how digital security risk management can affect other people, whether the respondent has the necessary skills to understand the digital security risk, the means of acquiring skills, and whether and where there is a skills gap.

---

8 The preparation of the pilot questionnaire considered the key concepts and definitions, measurement challenges, and indicators proposed in the document "Proposed draft indicators on digital security risk management practices in businesses" (OECD, 2017), the main methodological reference that guided the OECD project. An addendum to this work, entitled "Revision of Indicators for Measuring Digital Security Management Practices in Businesses," offered contributions to the original analytical framework and indicators based on the feedback of the OECD WP-SPDE and WP-MADE working groups. In addition, three survey questionnaires were used as methodological references for its design: the Community Survey on ICT Usage and E-Commerce in Enterprises (Eurostat, 2017), the United Kingdom Cyber Security Breaches Survey 2018 (Klahr et al., 2018), and the Canadian Survey of Cyber Security and Cybercrime (Statistics Canada, 2017).

DEVELOPMENT OF A QUESTIONNAIRE FOR MEASURING RISK MANAGEMENT PRACTICES

The Regional Center for Studies on the Development of the Information Society (Cetic.br) and the Brazilian National Computer Emergency Response Team (CERT.br), departments of the Brazilian Network Information Center (NIC.br), established a cooperation protocol with the OECD with the objective of building a data collection instrument, according to the specific activities detailed below:

- Review of questionnaires and reports on digital security and risks, aiming to integrate existing indicators, questions, and answer categories;
- Development of a preliminary version of the pilot questionnaire to be shared with the OECD Working Party on Security and Privacy in the Digital Economy (WP-SPDE)[9] and Working Party on Measurement and Analysis of the Digital Economy (WP-MADE);[10]
- Receiving feedback from working groups on proposed questionnaire modules, including concepts, definitions, question and answer categories, topic structure and flow, sequence of questions, filters, and wording;
- Conducting cognitive interviews, and preparing the final report with the analysis and recommendations for improving the questionnaire;
- Updating of the preliminary version based on cognitive interviews, and development of the final version of the questionnaire for discussion among working groups for validation.

The data collection instrument was developed and improved between March and April 2018 by the group composed of representatives from Cetic.br|NIC.br, CERT.br|NIC.br, and the OECD. The questionnaire was then submitted to a cognitive testing process, revised, and tested by the Federation

9 The OECD Working Party on Security and Privacy in the Digital Economy (SPDE) develops high-level public policy analyses and recommendations to help governments and other stakeholders ensure that digital security and privacy protection promote the development of the digital economy. More information at: https://www.oecd.org/sti/ieconomy/workingpartyonsecurityandprivacyinthedigitale-conomyspde.htm

10 The mandate of the OECD Working Party on Measurement and Analysis of the Digital Economy (MADE) is to conduct digital economy measurement and analyze the contribution of digital economy policies to economic performance and social outcomes. More information at: https://oecdgroups.oecd.org/Bodies/ShowBody-View.aspx?BodyID=5291&Lang=en&Book=True

of European Risk Management Associations (FERMA), from July to September 2018, gathering 80 interviews, mainly from risk managers of large enterprises from fifteen countries. As a result of the pilot projects, it was recommended that certain aspects of the survey were improved, such as the length of the questionnaire and specific adjustments to the formulation of questions and answers (OECD, 2019b).

QUALITATIVE APPROACH IN BRAZIL: COGNITIVE INTERVIEWS WITH BRAZILIAN ENTERPRISES

As part of the process of preparing the data collection instrument for the OECD project "Measuring Digital Security Risk Management Practices in Businesses," Cetic.br|NIC.br carried out a set of cognitive interviews[11] with Brazilian enterprises in order to assess the suitability of the questionnaire to the national context and its applicability in small, medium and large enterprises. They also sought to identify any sensitivity related to the questions, as well as to ensure that the questions were appropriate for the target audience (OECD, 2019b). In addition to providing information for the review of the OECD questionnaire, the results of this step were used by Cetic.br|NIC.br as input for carrying out a qualitative analysis on digital security risk management among 16 Brazilian enterprises.

QUALITATIVE METHODOLOGY: RESPONDENTS AND DATA PROCESSING

From March 26 to April 11, 2018, Cetic.br|NIC.br conducted 16 face-to-face cognitive interviews[12] with employed persons in enterprises of different sizes,[13] economic activities and geographic locations, in three municipalities in Brazil – São Paulo,

11 Cognitive interviews assess survey questions using various techniques to ascertain how respondents understand the questions and how they arrive, through their own cognitive reasoning, at their answers (Groves et al., 2009). It is particularly useful for evaluating new questions and identifying possible sources of error before applying survey questionnaires on-site, as well as evaluating issues of translation and adaptation of international questionnaires, identifying any sensitivities to specific questions and ensuring that they are appropriate for each target population.

12 When it was not possible to conduct interviews in prepared rooms, respondents were contacted at their workplace. All interviews – whether in the interview room or at their workplace – were fully recorded, and internationally accepted ethical recommendations were applied.

13 The concept of enterprise size considers small (10 to 49 employees), medium (50 to 249 employees) and large (250 or more employees) enterprises. Microenterprises, which have one to nine employees, were not included in the scope of cognitive tests.

Recife, and Porto Alegre (Table 1).[14] These locations were selected to ensure regional diversity among respondents. The type of economic activity of the interviewed enterprises was classified according to the National Classification of Economic Activities (CNAE 2.0) and refers only to enterprises legally constituted in Brazil, categorized and registered in official records. Furthermore, although the questionnaire was aimed at small and medium-sized enterprises (SME), five large enterprises were interviewed in order to understand the influence of the size and complexity of these organizations on the general understanding of the questionnaire.

TABLE 1 – CHARACTERISTICS OF THE ENTERPRISES SELECTED FOR COGNITIVE INTERVIEWS

CITY	ECONOMIC SECTOR	SIZE	POSITION OF THE RESPONDENT
São Paulo	Transportation and storage	Large	Risk Director
São Paulo	Real estate activities	Large	IT Director
São Paulo	Accommodation and food service activities	Large	IT Supervisor
São Paulo	Construction	Large	IT Manager
Recife	Wholesale and retail trade	Large	IT Manager
São Paulo	Arts, entertainment, and recreation	Medium	IT Coordinator
São Paulo	Real estate activities	Medium	IT and Infrastructure Coordinator
São Paulo	Transportation and storage	Medium	Administrative Manager
São Paulo	Information and communication	Medium	Financial Manager
Porto Alegre	Construction	Medium	IT and Administrative Manager
São Paulo	Information and communication	Small	Infrastructure Manager
São Paulo	Arts, entertainment, and recreation	Small	Operations Manager
São Paulo	Arts, entertainment, and recreation	Small	Project Manager
São Paulo	Retail	Small	Owner
Recife	Real estate activities	Small	Owner
Porto Alegre	Accommodation and food service activities	Small	Owner

SOURCE: PREPARED BY THE AUTHORS.

The people selected for the interviews were formally employed by the enterprises.[15] Initially, professionals who had a role in managing the economic and social risks faced by the organization, such as risk managers, were sought. If there was no employee who had been explicitly assigned for risk man-

14 Cetic.br|NIC.br had the support of IBOPE Inteligência for prospecting and contacting respondents and for the logistics of face-to-face and remote interviews.

15 The concept of employees refers to those remunerated directly by the enterprise, with or without an employment contract. The number of employees included wage earners, freelancers paid directly by the enterprise, employees and associates, family members, and temporary workers. Third parties and consultants were not included.

agement in the enterprise, the interview was conducted with owners, Chief Executive Officers (CEO), managers or other employees who had an overview of the economic or commercial status of the enterprise.[16]

The analysis of the empirical material was based on a procedure to code the transcripts of cognitive interviews, which allowed classifying and organizing the collected contents, comparing answers and discursive contents of different respondents, as well as measuring references to certain topics and crossing them with specific attributes of the universe of respondents. It is important to highlight that, although the OECD framework guided the preparation of the questionnaire and helped in the analysis of the results, the material resulting from the cognitive interviews was analyzed considering characteristics of the Brazilian context[17] and including new categorizations and groupings of analysis dimensions.

MANAGEMENT OF DIGITAL SECURITY RISKS AMONG BRAZILIAN ENTERPRISES

Below is an overview of DSRM statistical indicators among Brazilian enterprises based on data collected by the ICT Enterprises 2019 survey (NIC.br, 2019) for the first time, with the objective of providing a general context on this topic in the country.[18]

A BRIEF CONTEXTUALIZATION OF DSRM IN BRAZIL: DATA FROM THE ICT ENTERPRISES SURVEY

According to data from the ICT Enterprises 2019 survey (NIC.br, 2019), 41% of enterprises have some type of digital security policy, and the most prevalent are medium (63%) and large (74%) enterprises. As shown in Chart 1, although

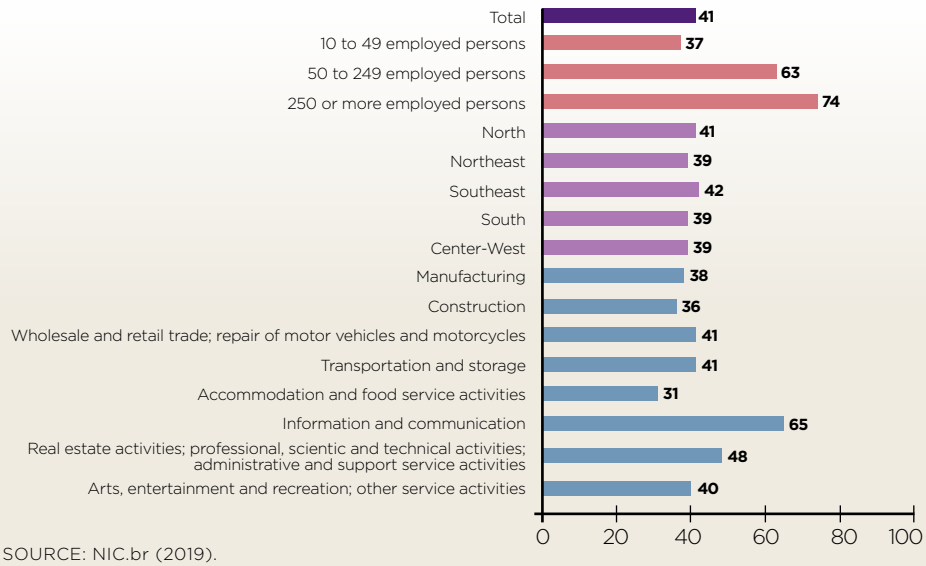
16 In the case of Brazil, it is worth noting that several respondents considered digital security risks primarily as a technical issue and indicated that technical staff (such as IT managers) were the best people in their enterprises to answer questions about digital security risk management decisions.

17 Profile of the enterprises: in addition to the approach adopted, based on the OECD framework, the specific context of each enterprise was considered relevant for the understanding of digital security risk management. Thus, the five dimensions selected to carry out the analysis, as well as the categories for the corresponding coding, were adapted to make sense to the reality of Brazilian enterprises, including, for example, the barriers for digital security risk management.

18 The ICT Enterprises survey, conducted every two years by Cetic.br|NIC.br, aims to measure the access and use of ICT in Brazilian enterprises with 10 or more employed persons. More information available at https://cetic.br/en/pesquisa/empresas/

there are no differences by region of the country, the market segment with most enterprises that have some type of digital security policy is Information and Communication (65%), characterized by an intensive use of ICT and by delivery of digital products or services.

CHART 1 – ENTERPRISES THAT HAVE A DIGITAL SECURITY POLICY
Total number of enterprises with Internet access (%)

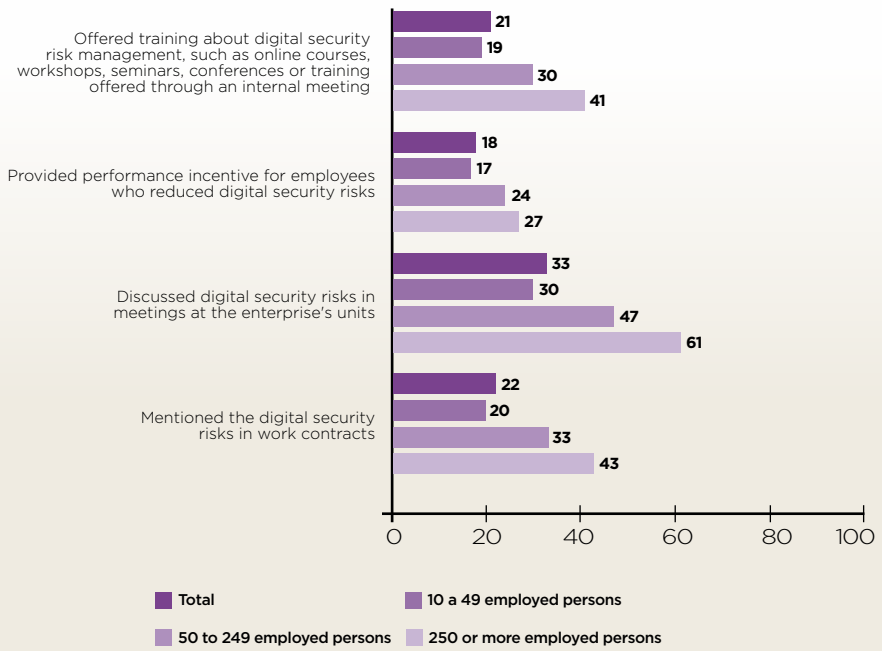


SOURCE: NIC.br (2019).

The ICT Enterprises 2019 survey (NIC.br, 2019) also sought to understand how the enterprises' risk management policies translate into practices aimed at mitigating digital security risks. In this regard, the data show that few enterprises implement actions to inform employees about digital risks, such as training (21%) or discussion about this topic in their meetings (33%). In addition, the percentage of enterprises that reported, for example, that they have work contracts that mention digital security (22%) or performance incentives for reducing digital risk (18%) is low. In general, actions aimed at digital security are more present in large enterprises, with discussion during meetings being the most mentioned, as it is adopted by 61% of large enterprises.

CHART 2 – ENTERPRISES, BY DIGITAL SECURITY PRACTICES

Total number of enterprises with Internet access (%)



SOURCE: NIC.br (2019).

The data collected by the ICT Enterprises 2019 survey (NIC.br, 2019) reveal an incipient presence of digital security policies or practices among Brazilian enterprises of all sizes, especially in small enterprises. These topics are explored below, based on the qualitative approach conducted with selected Brazilian enterprises.

MAIN HIGHLIGHTS OF THE ANALYSIS OF QUALITATIVE INTERVIEWS WITH BRAZILIAN ENTERPRISES

Based on the OECD framework, five dimensions were established to guide the analysis of the cognitive interviews carried out with the 16 Brazilian enterprises. The main highlights will be presented for each of the following analytical dimensions: *(i)* View on (the management of) digital risk and

risk exposure; *(ii)* Digital risk analysis and assessment processes; *(iii)* Acceptable level of digital risk and consequences of the incidents; *(iv)* Digital risk reduction and transfer practices; and *(v)* Corporate structure and challenges for digital security risk management.

View on (the management of) digital risk and risk exposure

The OECD framework seeks to ascertain **whether** and **how** digital security risk management (DSRM) is integrated into the risk management practices of enterprises. From this perspective, digital risk is not essentially distinct from other types of risks, thus it should be the object of proactive decision-making at the managerial level (Jalali, 2018), while DSRM must be integrated into the broader risk management framework (OECD, 2015). In the Brazilian context, however, SME do not always have a department, an area or a person responsible for the risk management of the entire enterprise, and digital security is not considered exactly a management area either.

Thus, when respondents from the Brazilian enterprises interviewed were consulted about risk management specifically in the digital context, the risks mentioned often related to other types of risks, such as financial, operational, and hiring. This vision of digital security risk management – along with other elements discussed below – highlights the fact that issues related to digital security, both in small, medium and even in some large enterprises interviewed, are limited to the technical area or related to the management of incidents.

"Well, I understand risk management as something very related to computers, something closely related to information. [...] I understand this as something linked to corporate governance, to risk audits, something related to a larger enterprise, to a larger business, to compliance [...] a series of standards that have to be met; otherwise, this may result in fines."

(OWNER, SMALL ENTERPRISE)

This view of digital security as a technical issue implies that the focus of attention is on the security risk for systems and networks, a view that is reinforced by the examples provided by respondents – such as data breaches and recent cases of ransomware attacks. The economic and social consequences of the incidents – financial and reputation losses, loss of business

opportunities, competitiveness, and trust, and the impact on privacy – do not play a central role on the agenda of the leaders of the interviewed enterprises.

DSRM assumes the existence of coordinated actions to handle digital security risks and maximize opportunities, as well as their integration into an overall framework to manage risks to the organization's activities (OECD, 2015). Furthermore, it is based on a systematic and flexible set of cyclical processes that ensure that DSRM measures are appropriate to and commensurate with the risk and economic and social objectives at stake (OECD, 2015). If the views of enterprises regarding risk management do not vary much according to the economic sector and/or degree of digitalization, the size and internationalization of an enterprise appear to be relevant variables for understanding the topic, as the only enterprises that reported that they have digital security risk management processes, or at least rely on a reflective risk assessment process, were the largest multinational enterprises.

It was found that, in addition to the fact that DSRM is not part of the routine of small and medium-sized enterprises, the concept of digital risk is not clear to many respondents. The difficulty of naming and understanding digital risks does not depend on the digital maturity and economic sector of the enterprise in question. In the interviews, it was seen that risk is mostly associated with information leaks regarding the enterprise.[19] Across all profiles of the enterprises interviewed, there is great concern that employees and/or third parties have improper access to e-mails, the Internet, to situations involving the loss and leak of enterprise information, to data hijacking, and to the invasion of computers and servers.

In relation to these concerns, particularly with regard to data hijacking, it is important to note that ransomware[20] is one of the most widespread attacks on digital security and represents a serious threat to enterprises of any size, but especially

19 It is important to highlight that the interviews were conducted in 2018, after the WannaCry attack, the largest ransomware attack in history, which affected more than 200,000 systems in 150 countries.

20 "After becoming infected by malware by clicking on a link or downloading and opening a file, the unsuspecting user finds that they are unable to boot their programs, or access their files. A ransom note informs them that their files are now encrypted and a payment is required to release them. Meanwhile, the ransomware has spread throughout the enterprise network, encrypting as it goes." (Stuart, 2016, para. 2).

to SME (Stuart, 2016). However, mitigation best practices apply to everyone and, if carried out correctly, they have positive effects that go far beyond ransomware. In the interviews, the examples of risks mentioned were accompanied by what is believed to be one of the most effective measures to reduce them: backing up data, either on proprietary servers, in the cloud or by hiring a service to do so. This is also seen in the two most mature enterprises in terms of digital security, one of which, according to the respondent, had "duplicate" and even "triplicate" backups, and a solid business continuity plan in the area of information technology.

"[...] we enter encrypted data [...] it is more difficult for us to have an invasion, to have data from customers and even employees leak [...]. The availability, the loss of information, we usually work with backups, [...] especially in the case of essential services for enterprises, IP telephony, for example, ours is IP telephony, server mailbox is very important, part of a file server."

(OPERATIONS MANAGER, SMALL ENTERPRISE)

Although small enterprises apply digital security risk management practices – in this case, to reduce risks –, the reports indicate their isolation in relation to technological decisions, which are limited to "IT staff." Given that measures to reduce digital security risk can have negative effects on the economic and social activities they are supposed to protect – affecting innovation processes, performance etc. –, the existence of risk management processes that seek to reduce risk to an acceptable level without compromising the enterprise's operations is necessary. This consideration, adopted by the leadership of the enterprise, was rarely reported during the interviews.

The only enterprise interviewed that mentioned options to handle risk – that is, to analyze and reduce the risk, and mitigate the consequences of the incident – was a large multinational enterprise. For the respondent of this enterprise, risks are not considered strictly negative, as they can also bring gains for the enterprise. In this regard, a point to be highlighted is that the very notion of risk assumes exploring uncertainty – innovating implies taking risks (and digital security aims to increase the likelihood of success of economic and social activities) (OECD, 2015). That is, although "risk" usually only captures the harmful effects of uncertainty, it can also have positive effects and benefit activities. However, the benefi-

cial effect of uncertainty is often called "opportunity" rather than risk. The relationship between risk and opportunity is important, as DSRM can also be used to create value, since it systematically detects and takes advantage of uncertainties to drive innovation (OECD, 2015). However, if it is true that some organizations become stronger, and if the most resilient organizations in digital security can respond to an incident, fix vulnerabilities, and apply lessons learned to future strategies, a key element of their resilience is governance, a task that is the responsibility of the organization's leadership, and not only of the technical team (EIU, 2018).

"In risk management, you have positive risks and negative risks, right? Suddenly, there is an opportunity for a positive risk that I can bring to the organization and we can review some situations that could lead to a gain for the enterprise. [...]. Risk management is not just a loss of business."

(RISK DIRECTOR, LARGE ENTERPRISE)

Although there is great concern regarding access to confidential information, the main point of attention is related to the use of this information by competitors or employees. Although some respondents mentioned the importance of compliance actions, the concern with the protection of personal data of business partners was not mentioned in the interviews.[21] Ultimately, respondents recognize risks that generate financial loss more immediately. It should be noted that theft of trade secrets[22] may lead to significant opportunity costs, negative impacts on innovation, increased security expenses, and reputational damage (PwC, 2019), especially when it comes to SME which are, at the same time, more vulnerable targets to this type of attack.

"The enterprise's website was invaded, a lot of advertising was added to it [...]. The risk is of losing sales, the risk is of losing the partnership with my distributor, my manufacturer. [...]. It is a matter of information [...]. They are competitors, they are in the same market, so we have to maintain confidentiality."

(FINANCIAL AND INFRASTRUCTURE MANAGER, MEDIUM ENTERPRISE)

It was noted that in enterprises with diverse profiles, risk was associated with something that originates from the en-

21 At the time of the interviews, the EU General Data Protection Regulation (GDPR) of the and the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais – LGPD) were not yet part of media debates.

22 The knowledge and information that enterprises treat as confidential are valuable trade secrets, and they are considered fundamental assets for their competitive advantage in the market. A significant number of cyber intrusions target valuable knowledge and information such as details about the business, know-how, and technology that enterprises treat as confidential.

terprise itself, that is, an internal risk: digital security, in this sense, is considered the establishment of rules for what employees can or cannot do. This makes employee control a key issue to manage these risks – for example, a very common issue mentioned by respondents is the potential misuse of USB flash drives by employees, with the aim of appropriating information that would benefit them. This understanding of "internal risk," which is often linked to employee behavior, results in management practices based on control, which contrasts with management that encourages employee responsibility and fosters awareness and training. To keep the digital security ecosystem healthy, employees need to be trained to understand what safe behaviors mean in terms of digital security and how to avoid unnecessary risks (Worthy, 2017).

"[...] it is controlling everything that is in my network, everything that comes in and out, so I must have control over it. I have a tool today that helps me with this control, [...] mainly customer information. [...] today, if one of my employees uses a USB flash drive [...] this is my part in digital risk, to control the information that comes in and out of my network."

(IT AND INFRASTRUCTURE COORDINATOR, MEDIUM ENTERPRISE)

Also in relation to this topic, for respondents from small enterprises, risk is seen as something internal that can be "physically" accessed. In this regard, it is worth noting that digital security can be compromised by any incident that affects the CIA triad of hardware, software, networks and/or data on which an enterprise's economic and social activities rely. Potential events can be intentional or unintentional threats (such as human errors or natural events) that take advantage of vulnerabilities – for example, errors (bugs) in hardware, software or networks; lack of training; insufficient protection, whether digital (firewalls) or physical (cameras and locks in the data center); as well as inadequate procedures (backup processes or disaster recovery plans).

Digital risk analysis and assessment processes

Digital security risk management assumes that risks are identified (any possible risks, bearing in mind the dynamic and changing nature of digital risks), analyzed (its likelihood to affect the enterprise itself and potential impacts), and evaluated (from which actions are taken, considering the organization's risk appetite) (OECD, 2015).

However, in the interviews, there was no mention of processes established to identify risks, to analyze any consequences – in relation to the enterprise's vulnerabilities – or to decide the course of action based on an assessment. Regarding the latter, it was found that only the most mature enterprise in terms of DSRM – a large multinational enterprise – has ongoing processes with a predefined periodicity to decide how much risk should be assumed, reduced, transferred, and avoided (see p. 128), associating this situation with the organization's risk appetite. Except for this enterprise, the four strategies to handle risk were not identified by the respondents.

"We do not have a process because we make these decisions in board meetings. But they are not written, somebody brings it up, and another person approves it. No, we have a process that is, I would say 50% mature, but is not formal. People are aware of what happens, but this is not written down."

(IT DIRECTOR, LARGE ENTERPRISE)

It should be noted that decision-making regarding risk management strategies derives from its assessment process. The measurement of how much risk the organization is willing to accept in order to carry out an activity is known as its "risk appetite," which depends on many factors, such as the type of activity and its objectives, the organization's culture, market conditions etc. Unless the risk is fully accepted or avoided, a decision must be made on how to reduce it to an acceptable level or transfer it (OECD, 2015). Therefore, the assessment process is crucial to manage risk properly.

The perception of digital risks as an exclusively technical issue seems to lead to uncoordinated levels of DSRM practices. In fact, in the interviews, there was no evidence of enterprises with structured processes that consider the results of digital risk assessment in their management actions. On the contrary, it was observed that the actions implemented are usually reactive, that is, taken after the organization has suffered an incident. In other words, risk reduction practices, as well as information sharing and reported internal awareness actions, were directly associated with the occurrence of specific security incidents and not with prior risk management. Even when activities developed by the enterprises in terms of digital risk assessment were mentioned, they indicated that these activities usually take place at general meetings and not on a regular basis.

This reactive work goes against the dynamic nature of risk, which must be assessed and addressed on an ongoing basis, as part of a continuous risk management cycle, to ensure that existing risks are properly managed and any new risks are identified and successfully mitigated. Digital risks require enterprises to be proactive in developing digital security capabilities: if an organization has strong digital security protections and protocols before a breach, it can recover faster and have lower costs from digital attacks (Jalali, 2018). Likewise, clear digital security policies need to be defined and regularly reviewed to ensure that risks are addressed, and threats are minimized (Worthy, 2017).

"It follows the market. Let's say, you know there is a cyberattack and then you kind of monitor it, about every three months. Because you never know when a cyberattack will happen. [...]. It is on demand. [...] cyberattacks usually occur from Friday to Sunday. These are periods when there is no one there physically analyzing what is happening. So, theoretically, these are the days that you are more alert, it can happen."
(IT AND INFRASTRUCTURE COORDINATOR, MEDIUM ENTERPRISE)

The previous quote also reflects the low maturity of enterprises – observed during the interviews – in terms of structured DSRM policies. Thus, it was found that only the two largest enterprises interviewed, both multinationals, have a formal written policy that can be considered DSRM.

It is noteworthy that, although several respondents have stated that there is a risk management policy in their organizations, when explaining what it was about, they cited meeting minutes and, mainly, "manuals," behavioral guidelines, and/or codes of ethics for employees (with details on monitoring network access, use of personal e-mails, use of USB flash drives, and access to the enterprise's contacts). Some enterprises also mentioned the disclosure of a practical guide on the use of electronic devices by employees. The assimilation of the DSRM policy with the rules of internal behavior – considered as a "Human resources affair" – reflects the understanding that respondents have about what constitutes a digital security risk, which, in many cases, is conceived as an internal risk, subject to improper actions by employees that undermine the enterprise.

It is noteworthy that some respondents consider they have informal means of disseminating best practices, which shows that DSRM follows the general behavior rules of the organiza-

tion – in these cases, it is a set of recommended practices and not a formal policy of the enterprise. Even when the goal of "best practices" is to guide employee behavior to avoid digital incidents – understood as the enterprise's DSRM policy – respondents believe that the policy encompasses the entire organization and not just its digital environment. In other words, the policy is understood as a set of procedures that cover all situations in the enterprise, from the relationship among employees to the correct way to use the Internet, how to ensure data protection, and how to report and handle security incidents. This general policy includes not only DSRM, but also other aspects that are important for the good functioning of the organization.

"It is written in the manual, on a page dedicated exclusively to security policy."
"Is this the digital security policy? [...] What does it say?"
"What is allowed in access, what is allowed in relation to the use of resources, printing, not doing other work during working hours, exactly as if it were a manual on how to use IT with the same items that we created on that basis [...] but there they make it clear what cannot be done. We described the main issues: Internet access, the use of resources, not sharing your passwords with anyone, not copying any content, that all work contents must be stored in the department folders."
(IT AND ADMINISTRATIVE MANAGER, MEDIUM ENTERPRISE)

Some respondents justified not having a policy in place because of the size of the enterprise, that is, a policy is not necessary since there are no problems related to digital security in small organizations. Others attributed this absence to the dynamic nature of digital risks, which would require changes in their policies every time new issues arise.

The two enterprises that showed greater maturity in terms of digital security risk management were the largest multinational ones, as mentioned. Therefore, it is worth noting that the DSRM policy available in both cases is an "imported" policy that has been adapted to the Brazilian context.

"Yes, you have simple things like passwords, you cannot keep them in a drawer. There are internal trainings to remind us of the obvious. [...] It comes from abroad, it is a German enterprise, so, of course, we make some adjustments. [...] there is even a very robust training for all employees and it is mandatory, it is called [name of the training program]. [...] It is always customized to the local context, but there is not much room for changes. [...] The entire policy can be accessed here, in our public folder."
(RISK DIRECTOR, LARGE ENTERPRISE)

Acceptable level of digital risk and consequences of the incidents

The data collected in the interviews with the enterprises show that, in the absence of structured processes on the topic, the definition of how much risk is tolerable is made by IT managers, project managers, and/or information security managers. Therefore, this is a technical decision and not necessarily a strategic one – with the exception of the two largest multinational enterprises, where the person responsible for establishing the enterprise's "risk appetite" is the president or CEO.

Even if technical experts understand the possible threats, vulnerabilities, incidents, and options for digital risk reduction, enterprise managers are in a much better position to establish the "risk appetite" of the organization, assess any consequences of risk according to the economic and social objectives, and ensure that security measures do not undermine these activities or reduce the potential of ICT to innovate and contribute to competitiveness. Therefore, ideally, both should work together, whereas risk decisions and management must ultimately be undertaken by the enterprise's decision-makers rather than delegated to technical experts (OECD, 2015; Jalali, 2018). In this regard, it is worth noting that in the interviews, it was clear that the acceptable level of risk is a concept that is not easily understood by the respondents, and there seems to be no conscious process on how much risk to take.

In the enterprises interviewed, there was no assessment mechanism to establish the acceptable level of risk, which could be determined based on structured risk assessment processes. The absence of these mechanisms reflects the precariousness of digital security risk governance, given that risk assessment, as an ongoing process, must establish how much risk is accepted, reduced, and transferred – a discussion that is absent in the practice of the Brazilian enterprises interviewed. The risk assessment process is important because it allows taking into consideration the potential consequences of threats, combined with the vulnerabilities in economic and social activities at stake; the decision-making for addressing risk is also informed in the process (OECD, 2015). Therefore, the decision on the handling of risk must reduce the risk to an acceptable level in relation to

economic and social benefits – that is, innovating and capitalizing on the use of technologies in businesses.

Even though there are no structured processes to handle risk, when asked about the topic, many of the respondents said that the level of digital security risk is acceptable if it does not compromise the functioning of the business. In this regard, the total or partial downtime of the enterprise – whether for hours or days – is one of the main consequences that respondents from small and large enterprises reported and the one that defines how much risk to accept.

> "When the system is down [...]. It is losing business, it is losing revenues, I am not sending something to the government, which could generate a fine. These are all consequences of digital risk."
>
> (IT DIRECTOR, LARGE ENTERPRISE)

Managers are responsible for deciding how much risk to accept and for taking into account the possible consequences of any digital security incident. In practice, these issues are delegated, on purpose or by default, to the IT area. According to Jalali (2018), this is possibly due to the fact that leaders fail to perceive the complexity and importance of digital security. According to the author, managers and/or leaders will hardly invest time and resources to defend or recover something that, to them, seems unlikely to sustain an attack – an assessment generally based on perceptual characteristics. In this regard, a rational decision-maker invests in information security if the investment leads to positive revenues or if the investment costs less than the risk it eliminates. Difficulties in measuring the costs – and understanding indirect costs – of potential digital incidents, as well as the benefits brought by these investments, obscure the view of the decision-maker: in addition to a high level of complexity, as these investments often involve intangible factors such as trust and willingness, there is also a lack of historical data,[23] effective metrics related to digital attacks, and knowledge about the type and range of uncertainties involved (Jalali, 2018; Richmond, 2013).

---

23 The important role played by the Computer Security Incident Response Teams (CSIRTs) such as CERT.br|NIC.br is noteworthy. However, as presented on pages 150-151, sharing information about digital security incidents is not a practice found in the enterprises interviewed, as only one person interviewed mentioned being familiar with CERT.br|NIC.br.

Similar to the difficulty of respondents in understanding the acceptable level of risk, respondents also found it difficult to recognize the potential consequences of digital incidents that the enterprise could suffer. Even when access to confidential customer information was mentioned, including leaks, the potential consequences of this risk were associated with economic losses for the enterprise – arising from the use of this information by the competition or the employees themselves –, without mentioning the longer-lasting implications in terms of violating the privacy of such third-party information or staining the enterprise's reputation.

Digital risk reduction and transfer practices

Although most of the interviewed enterprises do not have ongoing and systematic risk management cycles or processes to determine the enterprise's risk exposure and appetite that leads to decisions on the risk reduction measures to be implemented (OECD, 2019a), it is possible to identify isolated risk reduction practices that often rely on individual initiatives of those responsible for the IT area.

"Look, I did that only after I got robbed."
"Yeah? Ok. Is there a predefined periodicity, is it event-based?"
"(Laughter). This should not be the case, but I think I am now more concerned about at least doing the maintenance of computers more often, at least every two months."
"*What does that involve? Checking if they are working, if the antivirus is on?*"
"If the antivirus is on, if there is a history, if there is quarantine, anyway, running scanning software in it."

(OWNER, SMALL ENTERPRISE)

Having a backup is the main practice mentioned by respondents, both from SME and large enterprises. Similarly, updating antivirus and servers is considered a key protective measure against digital risks. The care to be taken with passwords and access to websites is also mentioned, as it becomes part of the code of conduct disseminated – usually informally – to the organization's employees, especially at the operational and technical levels.

At this point it is worth revisiting the very concept of vulnerability, which relates to the weaknesses exploited by a player and comprises, for example, errors (bugs) in hardware, software, or networks; lack of training; insufficient protection, whether digital (firewalls) or physical (cameras and locks in

the data center); as well as inadequate procedures (backup processes or disaster recovery plans). However, evidence indicates that most digital security breaches result from human vulnerabilities[24] more often than technology or process failures, such as phishing, ransomware and other malware, business e-mail compromise (BEC), and wire transfer fraud (EIU, 2019). Therefore, although the reported practices are extremely important to reduce the risk of attacks, the disconnection of these practices from an established policy and/or process is reflected, for example, in the lack of formal procedures for the qualification of employees across the organization.

Also, most enterprises, regardless of size, have emphasized the measures and precautions taken to control employee behavior, but not so much for potential human error as for malicious acts. This concern is reflected in the "ban on using USB flash drives to control incoming and outgoing information," according to both the IT coordinator of a medium enterprise and the IT supervisor of a large enterprise. This situation creates a paradox: while the main risk reduction measures implemented aim to mitigate human vulnerabilities, enterprise members' awareness and qualifications about digital security are limited and not part of the organization's routine. In this regard, while enterprises can introduce better security measures, such as two-factor authentication – which no respondent mentioned –, restrictions on Internet navigation, personal e-mail etc., they should, ultimately, rely on people to follow best practices and share information about incidents, which can help them anticipate and prevent similar events (EIU, 2019).

The interconnection of processes between a range of diverse organizations is such that none of them are protected from possible incidents that may occur with others, so the habit of sharing information about threats, vulnerabilities, incidents, and risk management practices or security measures is important to operationalize cooperation among stakeholders (OECD, 2019a) and achieve a healthy ecosystem. However, this practice

24 A study by The Economist Intelligence Unit (2019) found that although system misconfigurations and accidental exposures are the second most cited vulnerability, in addition to human vulnerabilities, they are all caused by human error: lost, stolen or otherwise hacked devices; unpatched software vulnerabilities; activity in an unsecured network or location, such as an airport or coffee shop; and lost or stolen usernames and/or passwords.

is not carried out systematically by any of the enterprises interviewed; respondents even react with surprise or suspicion, questioning why this would be beneficial to the enterprise. One respondent even argued that, as it is not a public or publicly traded enterprise, there is no obligation to share information about any incidents or security issues.

"[...] we are not obliged to disclose it, we are not listed on Bovespa[25] [...]. I know that it can have a negative impact on the enterprise if I say there has been a failure, ransomware, or something like that. [...] Outsourced enterprises have a contract with us that establish the confidentiality of information."

(IT SUPERVISOR, LARGE ENTERPRISE)

In cases where respondents stated that they share information about digital risks with third parties, this refers to sharing data with business partners. In this regard, the sharing of information is aimed at solving a problem with a partner or customer with whom interaction is necessary, that is, it is directly associated with the occurrence of an actual security incident and not with risk management.

"[...] I have had to tell franchise owners to take basic security measures in order to avoid an attack [...]. And IT vendors, too, because I needed them, right? They shared it with me, so I took all the measures based on what they told me and the business partners, in this case, my system partner with whom I share the data center and the network. I had to tell him to see if he was doing everything right, and then I found out that the other one was not because he had been attacked."

(PROJECT MANAGER, SMALL ENTERPRISE)

When it comes to risk transfer, given the absence of processes in place to assess how much risk will be accepted in relation to the potential consequences and how much will be reduced, there appears to be a widespread lack of knowledge about what this means. Some even think it is impossible to transfer risks, because even if a service is outsourced, this would still entail some risk.

"I cannot transfer this digital risk, I have to handle it, deal with it the best way I can. Even if I hire a partner, the risk is still all mine. [...] even if I transfer it, any invasion, any loss of data is still mine. Even if I have a partner, he will at most refund me a contractual fine. Only insurance can do it; if you have insurance, you can transfer the risk to a third party."

(IT DIRECTOR, LARGE ENTERPRISE)

25 Note: Stock exchange located in São Paulo, Brazil.

Having a backup in the cloud or with another enterprise, according to the respondents, would be a form of transferring risks, which is considered a "way to ensure that data is stored in a safe place," as "a guarantee that it is at a third party, that assures you that this data will be stored." On the other hand, for a large enterprise, "doing everything internally" and not "relying on third parties" are situations seen as a positive differential for the organization. Thus, it is worth noting that the logic that governs risk transfer, as one of the four options to handle risk, is to transfer the unwanted effects of uncertainty about the activity's objectives to another person, for example, by contract, such as through insurance (OECD, 2015).

With a well-established DSRM, digital risk insurance can be used to cover risks that the organization does not know how to handle or reduce. However, SME reported not being familiar with insurance for digital risks, and some were even incredulous about the possibility of having insurance cover the consequences of digital incidents. The respondent from a large enterprise said that he had thought about having insurance, but this was viewed with suspicion, as it does not cover the loss of data, the item considered by the enterprise to be the most important – in addition to the financial issue. The lack of insurance, on certain occasions, is attributed to its high cost, which demonstrates the non-prioritization of having insurance.

> "Thinking in financial terms, no [insurance coverage is not sufficient], depending on the insurance you have, but you do not lose only money. So, insurance is not an advantage for some things. [...] the basic one is expensive, and it ends up not covering everything we ask for. [...] So, we reached out to them a few times, and at that time the coverage was only financial. I did not have insurance; for me, the most important aspect is the data. The financial part is important too, but if there is no data coverage, I do not think anyone offers this type of coverage. [...] to recover data."
>
> (IT DIRECTOR, LARGE ENTERPRISE)

Enterprise structure and challenges for digital security risk management

When considering the structure of the enterprises that were interviewed, no specific departments for DSRM were reported, especially due to the size of the enterprise, according to the respondents, which would also justify the fact that digital security issues "do not apply" to it, making the DSRM a matter of larger organizations.

"I am too small for these things, I do it myself; on a day when I am not doing anything, I go and look at the computers and see how things are going. [...] [this item] does not apply to me. [...] Me and my father. [...] It is a family business, a small business, and you have to do everything. [...] two, three computers; two, three people are not so afraid, we do not handle databases, confidential information, we do not handle enterprise balance sheets [...] I do not have to worry so much about it, that is why I have not structured one, as I do not have the size to structure a digital security policy."

(OWNER, SMALL ENTERPRISE)

On top of that, most enterprises do not have written policies on the topic, especially SME.[26] When there are DSRM practices in place, they are merged into more routinized processes and are not recognized as originating from the risk assessment, as seen particularly in small enterprises or in enterprises where the business has little technological dependence. It is worth mentioning once again data from the ICT Enterprises 2019 survey (NIC.br, 2019), because even though there is universalization of Internet among Brazilian enterprises of all sizes and economic sectors, as well as an increase in its online exposure, and intensification of e-commerce, it is notable that there is no similar increase in concern about inherent digital security risks.

Enterprises that process credit cards online must comply with the Payment Card Industry Data Security Standard (PCI-DSS),[27] even if they are small, as customers' credit card data is handled, stored and/or transferred. This reflects the role played by legislation to encourage the adoption of digital security measures in organizations, as shown in the following quote of an enterprise with low maturity in terms of DSRM:

"[...] it is the second enterprise that performs most credit card transactions in the Northeast, and we are required to have PCI-DSS, it is a security standard for credit card enterprises."

(IT MANAGER, LARGE ENTERPRISE)

It is interesting to note that most respondents – IT managers or project managers – think it is important to develop DSRM – or, at least, certain risk reduction practices. In this regard, DSRM often depends on the willingness of the person in charge to take care of the IT area, that is, a person who is

26 As presented on page 145, in most cases, enterprises reported informal practices such as warnings or general rules about employee behavior.

27 Chapter 2 of this publication highlights the enterprise compliance issue in relation to digital security and presents some of the main laws on this matter.

"in the right place at the right time," as mentioned above. In some cases, this manager can get the board involved, which makes it possible to carry out or establish certain digital security processes or actions, as reflected in the quote of the IT supervisor of a large enterprise:

"Since 2014, IT started to get big here, it was an IT from [food sector], which normally does not pay much attention to technology, so in 2014, when I started working here, I brought along many things that I learned in other large enterprises [...] and also from my contact with the IT vice president, as we got closer, a lot of things from there started to be applied here. [...] Today it is not official, I do not make this measure official; I record it, voluntarily, there is nothing in writing stating that I should conduct this analysis."
(IT SUPERVISOR, LARGE ENTERPRISE)

In other cases, the decisions made by the board do not involve the analysis or requests made by the IT area and, given this "lack of interest" or prioritization by the leadership, respondents often need to work on persuading them about the need to perform a certain action, hire a service, or purchase a product for digital security purposes.

In this regard, it is important to take into consideration the difficulties in measuring the costs and benefits of investments in information security, which obscure the view of the decision-maker (Jalali, 2018; Richmond, 2013). Many enterprises are still not aware of the risks they are incurring, and their leaders tend to view digital security expenses as a cost rather than a desirable investment (PwC, 2019). The lack of prioritization of this topic is also reflected in the resources allocated to it: according to the interviews, the development of digital security management goes as far as the cost is perceived as low. When it starts to become expensive in the view of those in charge, the decision is to take the risk – either consciously or unconsciously.

"[...] IT is seen as an extremely expensive department. So, for me to be able to justify a new hire, to justify a new solution, I need a number [...]. Look, can you see it? There were these many threats [...]. If I do not have a chart that really brings a solution, showing that I need a better person, if I do not have an analysis done on paper, I cannot do it."
(IT AND INFRASTRUCTURE COORDINATOR, MEDIUM ENTERPRISE)

In addition to the financial issue, it is noted that digital security is not considered a cross-cutting issue, since training, when available, is something necessary only for technical employees and/or those in the IT area. In this regard,

enterprises need to make their own workforce aware of the topic and emphasize the importance of training for the entire team (PwC, 2019).

"[...] for the 80 employees who use the network, we have never done it, but in the IT area, the 7 employees, we have talked a lot about security issues, because we are required to do it by the control department, which is the enterprise's director, for the confidentiality of these files. There are a lot of different documents we handle in our area, but we do not share them with the rest of the enterprise, as they do not have access to these files, only the IT area. So, if one of these files leaks, it was someone from IT who did it, but this is a mistake, because everyone should be aware of it."

(IT COORDINATOR, MEDIUM ENTERPRISE)

The precarious level of training in enterprises is not related only to digital risk management, but also to risk management in general. It was found in the interviews that the training has a reactive character: when an incident occurs, even without significant consequences, an informal conversation or meeting takes place, in which digital security issues are addressed.

Reflecting the respondents' notion of digital security risk, training in DSRM is often associated with the code of conduct or ethics that employees sign upon joining the enterprise – the same codes that some respondents also considered as the DSRM policy available at the enterprise. In other words, digital risk is associated with something that can result from employee behavior, and in fact the scarce training is directed to them – and not to directors and/or leaders –; however, it involves only informal conversations and imposition of restrictions. Indeed, employees need to understand how their activity can present digital risks and the implications of that behavior; also, clear digital security policies must be defined and regularly reviewed to ensure that risks are addressed, and threats are minimized (Worthy, 2017).

"[...] every two months, we gather the team and do what we call 'brainstorming'; we present a situation that happened to keep them aware, and the suggestions [...] Precisely to understand it, because I cut the access [...] As we are smaller, and this is not defined by the size, I say that it is participatory management. If everyone is aware of the information, I think it gets a lot easier. [...] training for directors or managers [...] is not [...] a mistake, because directors are also subject to failure."

(INFRASTRUCTURE MANAGER, SMALL ENTERPRISE)

The role of enterprise leaders in the process of digital transformation is increasingly important in choosing paths to follow and defining goals associated not only with the business model in the digital economy, but especially with the manage-

ment of digital risks. Training the technical and management staff is important for enterprises to participate in discussion forums on the issues of digital transformation, characterized by being open to new ideas, new ways of working, and collaboration with other players. In this regard, there is a consensus that a greater effort in training on digital resilience is needed, both within the workforce and at the strategic level. A broader awareness of the complexity of digital security and training programs such as simulation models are increasingly needed so that managers can prepare for the reality of dealing with digital threats (Jalali, 2018).

FINAL CONSIDERATIONS

The growing digitalization of the economy entails relevant changes in the lives of enterprises and, along with them, a series of challenges to be faced in order to take advantage of the benefits brought by technological advances. Digital security is an issue that presents a double challenge – if, on the one hand, it is still an area that is under-prioritized by Brazilian enterprises, on the other hand, the scarcity of data on the matter contributes to the invisibility and lack of perception of the potential consequences that digital security incidents can cause in large, medium, or small enterprises.

Regarding the low availability of data, it is necessary to consider the various methodological difficulties related to the measurement of the digital security risk management presented, since this is an emerging, dynamic topic – due to the very nature of the risks –, as well as a complex one, which makes it indispensable to establish measurement frameworks to guide data collection. However, there is also a lack of prioritization of the matter on the measurement agenda, related to the low awareness on the topic.

On this last point, the data collected in cognitive interviews conducted with selected Brazilian enterprises revealed that, according to respondents, digital security is not given due attention by enterprise leaders, who often consider it a costly area, which is inconsistent with the reality of the enterprise, or of little importance. Therefore, issues related to digital security – and risk management itself – are limited to the technical area and are not incorporated into the core business of the enterprise.

Because of that, in the routine of the interviewed enterprises, the approach given to digital security is generally reactive after incidents occur, instead of having established processes to properly manage the risks, in order to assess them and decide on the best treatment strategies that meet the enterprise's needs, as well as formal policies, awareness, and training efforts involving all members of the organization.

As this topic is incipient and not well known, not only by the general public, but especially by the interviewed enterprises, it is essential to continue collecting data – both quantitative and qualitative – to make visible not only the potential gains from the digitalization of the economy, but also the problems associated with it.

REFERENCES

Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York, NY: W. W. Norton & Company.

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerization? *Technological Forecasting and Social Change, 114*(C), 254-280.

Groves, R., Fowler, F., Couper, M., Lepkowski, J., Singer, E., & Tourangeau, R. (2009). *Survey Methodology*. New York, NY: John Wiley and Sons.

Jalali, M. S. (2018). *The Trouble with Cybersecurity Management*. Retrieved from https://sloanreview.mit.edu/article/the-trouble-with-cybersecurity-management/?gclid=CjwKCAjwkJj6BRA-EiwA0ZVPVjF2ECyG4-fODvwkcrXZFTFnd34M9ZiYvubJwNzk1UBbcDEbehuZVBoCQl4QAvD_BwE

March, J. (1994). *A primer on decision making: how decisions happen.* New York, NY: The Free Press.

March, J. (2010). *The ambiguities of experience*. Ithaca, NY; London, UK: Cornell University Press.

March, J., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33*(11), 1404-1418.

Núcleo de Informação e Coordenação do Ponto BR (NIC.br). (2019). *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas Empresas Brasileiras - TIC Empresas 2019*. Retrieved from https://cetic.br/pt/pesquisa/empresas/indicadores/

Organisation for Economic Co-operation and Development (OECD). (2015). *Digital Security Risk Management for Economic and Social Prosperity*. Retrieved from https://www.oecd-ilibrary.org/docserver/9789264245471-en.pdf?expires=1598901438&id=id&accname=guest&checksum=50D91465F99DCCD1665A917270B5C2EF

Organisation for Economic Co-operation and Development (OECD). (2017, October 20). Proposed draft indicators on digital security risk management practices in businesses. *Working Party on Security and Privacy in the Digital Economy* (for Official Use). Paris, FR: DSTI/CDEP/SPDE.

Organisation for Economic Co-operation and Development (OECD). (2019a). Measuring Digital Security Risk Management Practices in Businesses. *OECD Digital Economy Papers, 283*, Paris, FR: OECD. Retrieved from https://www.oecd-ilibrary.org/science-and-technology/measuring-digital-security-risk-management-practices-in-businesses_7b93c1f1-en

Organisation for Economic Co-operation and Development (OECD). (2019b). *Measuring the Digital Transformation: A roadmap for the future*. Retrieved from https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm

Perrow, C. (1999). *Normal accidents: living with high risk technologies*. Princeton, NJ: Princeton University Press.

Pisano, G. (2017). Toward a prescriptive theory of dynamic capabilities: Connecting strategic choice, learning and competition. *Industrial and Corporate Change, 26*(5), 747-762.

PricewaterhouseCoopers (PwC). (2019). *Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber*. Retrieved from https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

Richmond, R. (2013). *Measuring the soft costs of cybercrime: a hard problem in need of a solution*. Retrieved from https://perspectives.eiu.com/technology-innovation/measuring-cost-cybercrime/article/measuring-soft-costs-cybercrime-hard-problem-need-solution

Schwab, K. (2016). *The Fourth Industrial Revolution: what it means, how to respond*. Retrieved from https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Srnicek, N. (2016). *Platform capitalism*. New York City, NY: Polity Books.

Stuart, A. (2016). *The rise and rise of ransomware*. Retrieved from https://eiuperspectives.economist.com/technology-innovation/rise-and-rise-ransomware

The Economist Intelligence Unit (EIU). (2018). Decode resiliency. *How boards can lead the cyber-resilient organisation*. Retrieved from https://eiuperspectives.economist.com/technology-innovation/how-boards-can-lead-cyber-resilient-organisation

The Economist Intelligence Unit (EIU). (2019). *Cyber insecurity: Managing threats from within*. Retrieved from https://eiuperspectives.economist.com/technology-innovation/cyber-insecurity-managing-threats-within

United Nations Conference on Trade and Development (UNCTAD). (2019). *Value creation and capture: implications for developing countries digital economy report 2019*. Retrieved from https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

Worthy, B. (2017). *What will it take for cyber safety to be recognised in the workplace?* Retrieved from https://perspectives.eiu.com/technology-innovation/what-will-it-take-cyber-safety-be-recognised-workplace

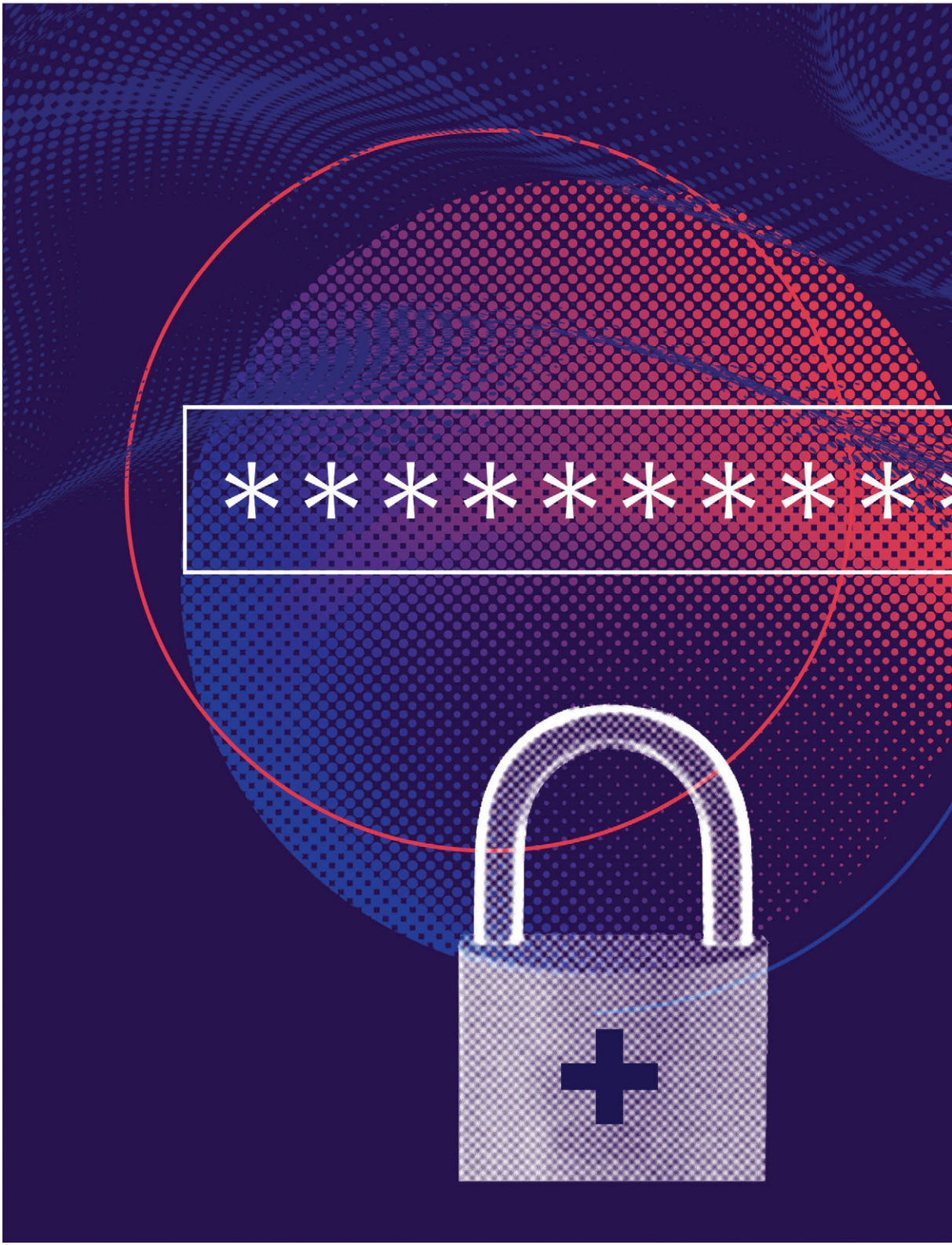
CONCLUSIONS

Regional context of cybersecurity

Jorge Alejandro Patiño[1] and Georgina Núñez[2]

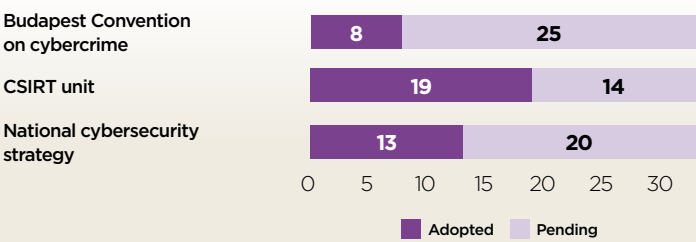
1 Jorge Alejandro Patiño is a specialist in the ICT sector at the Economic Commission for Latin America and the Caribbean (ECLAC), with over 15 years of experience in the field. He is co-author of several publications on digital technologies. He was Executive Director of the Bolivian Agency for the Development of the Information Society, a country code top level domain (ccTLD) administrator. He holds a degree in Economics from the Instituto Tecnológico y Estudios Superiores de Monterrey (ITESM) and a master's degree in Economics and Regulation of Public Services from the University of Barcelona.

2 Georgina Núñez is Regional Advisor linked to ECLAC's Division of Production, Productivity and Management since 2004, with a PhD in Economics from the Universidad Nacional Autónoma de Mexico, and a master's in International Economics and Politics from the Centro de Investigación y Docencia Económicas, A.C. (Mexico). She works on corporate governance issues, corporate debt issuance, competition policies, data protection and cybersecurity; and she is the author and co-author of several publications on these topics.



In recent years, some governments in Latin America and the Caribbean have improved the design of their legal frameworks and policies on cybersecurity: in 2015, while only six out of the thirty-three countries in Latin America and the Caribbean had a cybersecurity strategy, today that figure rose to thirteen (Lehuedé, 2020). The number of signatory countries to the Budapest Convention on Cybercrime, drawn up by the Council of Europe in 2004, increased from two to eight. Additionally, there is a Computer Security Incident Response Team (CSIRT) in nineteen of those countries (Lehuedé, 2020). However, as various indicators and reports emphasize, there is a variety of fields that require attention from governments, which include the adoption of new legal frameworks and their updating, but also issues related to technical and organizational capacity, as well as the development of the teams in charge of implementing cybersecurity strategies. According to the Global Cybersecurity Index (GCI) of the International Telecommunication Union (ITU), Latin America and the Caribbean, at an aggregate level, is ranked as the region of the world with the lowest degree of commitment to digital security, only preceded by Africa (ITU, 2019).

CHART 1 – FEATURES OF THE 2020 CYBERSECURITY FRAMEWORK, LATIN AMERICA AND THE CARIBBEAN (33 COUNTRIES)



SOURCE: ADAPTED FROM LEHUEDÉ (2020).

With respect to other metrics, the National Cyber Security Index[3] (NCSI), developed by the e-Governance Academy of the

3 The National Cybersecurity Index (NCSI) is a global index that measures the readiness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database of publicly available evidence materials and a tool for the development of capacities on national cybersecurity. For more information, visit: https://ncsi.ega.ee/

Government of Estonia, which compiles various indicators, suggests that there is a significant number of jurisdictions in the region that have adopted data protection frameworks and that have had a significant development in this area. Nonetheless, when cybersecurity domains are evaluated as general requirements for essential service operators or regular monitoring of cybersecurity measures, the results for the region are poor. With a few minor exceptions, there are no significant cybersecurity requirements targeting businesses, except for those driven by data protection (Table 1). Although the region has made progress in addressing cybersecurity, there are still lags in the regulation of essential services and critical infrastructure.

TABLE 1 – KEY CYBERSECURITY RULES RELATED TO DATA PROTECTION (SELECTED JURISDICTIONS)

	AR	BO	BR	CL*	CO	CR	DO	GT*	MX	PA	PY	PE	UY	VE
Data protection authority	✔	X	✔	X	✔	✔	X	X	✔	✔	X	✔	✔	X
Restriction on international transfers to other jurisdictions	✔	X	✔	X	✔	X	X	X	X	X	X	X	✔	X
Restrictions on transfers to data processors	✔	X	✔	✔	✔	X	X	X	✔	X	X	✔	✔	X
Sanctions	✔	✔	✔	✔	✔	✔	✔	X	✔	✔	✔	✔	✔	✔
Mandatory notification of breaches to authority and/or data subjects	X	X	✔	X	A	✔	X	X	✔	✔	X	X	✔	U
Mandatory DPOs	E	X	✔	X	✔	X	X	X	✔	X	X	E	✔	X
Mandatory DPIAs	✔	X	✔	X	R	X	X	X	✔	X	X	X	✔	X
Accountability	X	X	✔	X	✔	X	X	X	X	X	X	X	✔	X

SOURCE: LEHUEDÉ (2020).
NOTES (*): THESE JURISDICTIONS HAVE BILLS OF LAW CURRENTLY IN CONGRESS THAT INCLUDE SOME OF THESE MEASURES; E: EXCEPTIONALLY; R: RECOMMENDED; A: NOTIFICATION TO THE AUTHORITY ONLY; U: IT IS UNCLEAR WHO SHOULD BE NOTIFIED.

Regarding these services, the low level of cybersecurity preparedness of companies is noteworthy. Available data suggest that, while cyber risk is clearly a priority on the agenda of businesses in Latin America, progress in this area remains insufficient. Based on Marsh and Microsoft (2019, cited by Lehuedé, 2020), 16% to 22% of companies claim to understand, evaluate

and quantify cyber threats, while 12% to 20% are able to prevent cyber-attacks and only 7% to 18% manage such attacks and recover from them.

DIGITAL SECURITY IN THE CONTEXT OF INTERNATIONAL COOPERATION: A CONSENSUAL NATIONAL STRATEGY

In recent years, there has been an accelerated digitalization of the economies in the region, fueled by the current health crisis, which led to an increase in cyber threats and the need for a national cybersecurity strategy. In May alone, at the beginning of the COVID-19 pandemic, Google reported 18 million malware and phishing e-mails, in addition to 240 million spam[4] messages. There has been an increase in the understanding and awareness-raising on cyber-attacks and, therefore, the risks associated with the reputation of companies in this area have also become a highly valued asset worldwide.

Although certain key aspects of cybersecurity have been recognized as important in various fields and international agreements due to their high value as well as the potential damage, when reviewing the incorporation and implementation of these aspects in country policies, deficiencies can be noted. Some examples include: lack of identification of pieces of infrastructure (which should be considered critical), cybersecurity standards, monitoring rules, and accountability. In this sense, there are a number of aspects that range from the design and implementation of the cybersecurity policy, that must be adjusted.

Addressing the issue of digital security necessarily requires dialogue between the different social actors, including public and private, to guarantee effective governance and a coordinated effort at the national level for the implementation of a country's cybersecurity strategy. Likewise, it is essential to have various instruments in place for the coordination of actions regarding cybersecurity from the private sector. It may be the case that the companies that are responsible for critical infrastructure are in the hands of public operators, which could facilitate the adoption of security measures; however, in other

4 Retrieved from https://diarioti.com/covid-19-google-bloquea-18-millones-de-emails-fraudulentos-diarios/111571

areas, incentives and regulations that demand the implementation of actions with better defined guidelines are required.

Regional cooperation also plays an important role in advancing the definition of common parameters and motivating action. Since 2004, the region has had a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity,[5] adopted by the General Assembly of the Organization of American States (OAS). On the other hand, the Economic Commission for Latin America and the Caribbean (ECLAC) coordinates efforts from other forums for political dialogue, such as the Digital Agenda for Latin America and the Caribbean (eLAC2020),[6] which defines commitments on digital security (ECLAC, 2018). Work has also been carried out with different groups in the region for the construction of public-private dialogue and the planning of a national strategy, which is the case of the 8 member countries[7] of the Regional Telecommunications Technical Commission (COMTELCA).

Based on ECLAC's work, four key messages on digital security were identified: *(i)* the importance of a coordinated effort at the national level, in times of increasing digitalization of economies and increasing threats of attacks on national security information systems; *(ii)* the need to consider appropriate regulatory and institutional frameworks, and in the case of governments and companies, a public policy with clear guidelines on the protection of personal data, aligned with the strategy to face challenges; *(iii)* cooperation and multilateral effort, essential to face cyber threats; and, finally, *(iv)* the construction of a comprehensive and effective digital security strategy resulting from public-private partnerships.

---

5 The Comprehensive Inter-American Cybersecurity Strategy is based on the efforts and specialized knowledge of the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunication Commission (CITEL), and the Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA). The Strategy recognizes the need for all network and information system participants to be aware of their roles and responsibilities with respect to security, in order to create a culture of cybersecurity. More information at: http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp

6 The eLAC is a strategy aimed at 2020, which promotes the use of digital technologies as instruments for sustainable development. Its mission is to encourage the development of the digital ecosystem in Latin America and the Caribbean through a process of regional integration and cooperation, with the aim of strengthening digital policies that drive knowledge, inclusion and equality, innovation and environmental sustainability. More information at: https://www.cepal.org/es/proyectos/elac2020

7 The designated members are Mexico, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panama, and the Dominican Republic.

A cybersecurity strategy that has an effective governance requires a regulatory framework and effective response mechanisms, as well as the development and protection of critical infrastructure and systems. It also requires articulation with international cooperation to form a multilateral framework, as well as management of talent and technology to face challenges. In this regard, it is important to develop a holistic agenda that considers the different dimensions that compose a digital security and data security strategy.

The threat of attacks affects key sectors, such as: public and government services, food, fuel, transport, communications, and finance, which can entail significant risks for society as a whole, impact public treasury funds, threaten the electricity grid, telecommunications, and the supply of essential goods and services. These issues are very important for the defense of national security, the economy, health, public order, and politics.

A gradual increase is observed in both the complexity and the costs related to cyber-attacks on people, governments, companies, and information systems in general, which refer to the treatment of malicious programs (e.g., malware, spyware, data breaches, and ransomware), the theft of particularly sensitive data, data manipulation, attack on the functioning of computer systems (including those that control critical infrastructures), and extortion and cyber espionage programs.[8]

The response capacity of countries to cyber-attacks is becoming increasingly necessary, by virtue of depending, to a large extent, on the size, diversity and dynamism of the economic-social structures of the countries. It is crucial to respond to these attacks and mitigate their impacts, particularly on institutions, since they undermine governance when exposed to different types of risks:

- Attacks at different government levels (national, federal, regional, state, municipal) with economic consequences, in areas such as: income from multiple flows (from taxpayers), in multiple forms (income tax, VAT etc.), and the

8 According to the World Economic Forum (Morgan, 2020), it is estimated that by 2021 the economic impact of cybersecurity incidents could reach USD 6 trillion globally. The recent attack (ransomware) on the State Bank of Chile (Banco del Estado de Chile) represented the cost of almost USD 9 million to regain control over its platforms and data.

level of economic diversification to address these risks.[9]

- In terms of "political" structure, an attack can target the use of personal data for political purposes unlawfully obtained, and the use of social networks to influence voters by manipulating data via messages or through the use of platforms.
- Identity theft and fraud against public bodies.
- Construction of talent and technology in digital security that support the design and implementation of effective response mechanisms.

The international dimension and the need to generate a multilateral agreement is also essential, particularly in the cross-border flow of data regarding its protection, the protection of privacy and the consent of data owners. Associated with this dimension, it is important to mention the role of the framework provided by the Budapest Convention,[10] which defines in Article 32.b:

> Access to trans-border data. It is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual assistance under limited circumstances, including: *(i)* access publicly available (open source) stored computer data, and *(ii)* access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

An increasingly important issue to consider when designing a national cybersecurity strategy is the so-called data-opolies, which have become one of the main threats to digital security. Coordination of different government instances is necessary, associated with a limit to the power of data monopolies, across the economy. This includes limiting the concentration, not

9 For example, a PwC (2019) report for the European Commission indicates that the theft related to digital security of trade secrets in Europe in 2018 meant losses of EUR 60 billion for economic growth and almost 289 thousand lost jobs. The estimates that this same report makes for 2025 include an impact of one million lost jobs.

10 The Convention on Cybercrime, also known as the Budapest Convention, is an international treaty on criminal law and criminal procedural law signed within the scope of the Council of Europe to harmoniously define the crimes committed via the Internet and the way in which they fight them. Retrieved from https://rm.coe.int/16802fa428

only of big technology companies, which own digital platforms, but also of non-technology companies that have increased substantially in value due to growing access to data. The effects of the network, the lack of data portability, the user rights over their data, and the weak privacy protection help these monopolies to maintain a dominant position (Stucke, 2018). The higher concentration of data thus becomes an important incentive for massive cyber-attacks. Therefore, close coordination between those in charge of compliance with antitrust laws and those in charge of the protection of consumer privacy is essential to increase the safeguarding of conditions for effective competition, without affecting innovation.

FINAL CONSIDERATIONS

- A regional cybersecurity strategy has a double effect: raising people's awareness on the value of their data, so that they can protect it, and the possibility of having the authorities calculate, with greater precision, the scope of a digital ecosystem in terms of value, risks, and profitability.
- In Latin America, the issue of cybersecurity is fundamentally associated with data protection; therefore, the strengthening of its policy must necessarily include the cybersecurity dimension.
- In the present debate, the power of personal data and its growing value requires greater protection in face of multiple attacks. This is a central issue in international initiatives, which, among other things, seek that the user who accesses any digital platform can provide and control their information, which must remain duly protected.
- Public-private collaboration is essential for the success of an effective security policy for detecting risks associated with the use and misuse of data, mitigating the damage caused by an attack on privacy, and protecting data considered sensitive, personal, commercial, or industrial.
- A multilateral effort requires broad legal and institutional frameworks, which consider the varied forms and degrees of the impact of cyberattacks on companies, governments, and information systems. This should include aspects ranging from possible damage to a country's critical infrastructure, to the reach of malicious programs and a framework for the cross-border flow of data.

REFERENCES

Digital Agenda for Latin America and the Caribbean (eLAC). (2018, April 20). Cartagena de Indias Declaration. *Sixth Ministerial Conference on the Information Society of Latin America and the Caribbean*. Retrieved from https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_cartagena_de_indias_declaration.pdf

International Telecommunication Union (ITU). (2019). *Global Cybersecurity Index 2018*. Retrieved from https://www.itu-ilibrary.org/science-and-technology/global-cybersecurity-index-2018_pub/813559ed-en

Lehuedé, H. (2020). Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean. *Production Development series, 225* (LC/TS.2020/103). Santiago, CL: ECLAC.

Morgan, S. (2020, November 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine.* Sausalito, CA. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

PricewaterhouseCoopers Advisory SpA (PwC). (2019). *Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber*. Retrieved from https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

Stucke, M. (2018, March 27). Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data. *Harvard Business Review,* Boston, MA. Retrieved from https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data?mod=article_inline

United Nations
Educational, Scientific and
Cultural Organization

cetic.br

Regional Center for Studies on the
Development of the Information
Society under the auspices of UNESCO

cert.br

Computer Emergency
Response Team Brazil

nic.br

Brazilian Network
Information Center

cgi.br

Brazilian Internet
Steering Committee