CRITICAL INFRASTRUCTURE PROTECTION IN LATIN AMERICA AND THE CARIBBEAN 2018

OAS More rights for more people

Microsoft

CRITICAL INFRASTRUCTURE PROTECTION IN LATIN AMERICA AND THE CARIBBEAN 2018

CRITICAL INFRASTRUCTURE PROTECTION IN LATIN AMERICA AND THE CARIBBEAN 2018

CREDITS

Luis Almargo
Secretary General of the Organization of American States (OAS)

Tom Burt
Vice President and Deputy General Counsel for Digital Trust
Microsoft Corporation

OAS Technical Team
Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Carina Pietsch

Microsoft Technical Team
Andres Rengifo
Kaja Ciglic
Seema Kathuria

Contributors
Raúl Millán, Supervisor Specialist in Information Technology (Security), Unit of Security of Systems – TIGU, Executive VP of Technology and Information Technology, Panama Canal
Kaja Ciglic, Director, Government Cybersecurity Policy and Strategy, Microsoft
Hernán Vázquez, Information Technology Manager of the Regional Association of Companies in the Oil, Gas and Biofuels Sector in Latin America and the Caribbean (ARPEL)
Peter Burnett, Meridian Process

FOREWORD

Luis Almagro
Secretary General
Organization of American States

As a region, Latin America and Caribbean has experienced one of the fastest rates of Internet growth since the beginning of the century. The rate of Internet penetration in Latin America and the Caribbean is now estimated to be 65.1%, with more than400 million Internet Users.

While this growth has brought new opportunities for the region, the evolution of cyber-related threats in recent years has also heightened concerns regarding the actual and potential use of the Internet for illegal purposes. Recent data shows that the cost of cybercrime has reached $8 billion in Brazil, $3 billion in Mexico, and $464 million in Colombia.

Public and private critical infrastructure are also suffering from an increased number of cyber-attacks: owners and operators surveyed for the 2015 OAS-Trend Micro report Cybersecurity and Critical Infrastructure in the Americas reported a 53% increase of cyber incidents affecting their computer systems over the previous year.

Attacks on critical infrastructure have the potential to significantly disrupt the functioning of government and business alike and result in a ripple effect on the citizens of our nations.

These attacks could be magnified and even produce catastrophic losses if malicious actors decide to use components of a nation's critical infrastructure – systems and assets vital to security of a nation - as weapons of mass destruction.

The Organization of American States (OAS) is very pleased to present this report as a product of our ongoing partnership with Microsoft.

Collaboration with the private sector is a must for the protection of both Critical Infrastructure (CI) and Critical Information Infrastructure (CII). The OAS considers a multi-stakeholder approach, especially including the private sector, essential to the development of research and resources for the region and for the development of solutions for issues identified.

This Report presents an update on experiences in the region in relation to cyber-attacks against owners and operators of critical infrastructures and some of the best practices they have implemented to protect these vital assets.

Since 2004, the OAS has emphasized the "importance of developing a comprehensive strategy for protecting information infrastructure that adopts an integral, international and multidisciplinary approach". To this end, in 2015, the Fifth Regular Session of the Inter-American Committee against Terrorism (CICTE) issued a declaration on the "Protection of Critical Infrastructure from Emerging Threats," through which member states declared "their commitment to identifying and combating emerging terrorist threats, regardless of their origin or motivation, such as to critical infrastructure, and cybersecurity, among others and the need for private sector cooperation to prevent, develop resilience of critical infrastructure, and facilitate the resolution of terrorist and related crimes that are committed through global communication networks."

In this context, this Report has had the benefit of the participation of more than 28 of our 34 member states, and some of the positive conclusions from the results indicate that 53% of those that responded possess detection capabilities and keep records of these cyber events.

From a regional perspective however, one of the deficiencies identified was that only 49% of respondents responded positively to there being an agency with the responsibility for the protection of critical infrastructures. Further, when asked whether there were any incentives in place at the national level for Critical infrastructure operators to implement security measures, almost 78% indicated there were no such incentives in place, with a further 61% indicating there was no sector-specific regulation related to Critical Information Infrastructure Protection.

At the OAS, we focus our efforts on ensuring "more rights for more people." In the context of this study, that means protecting the rights of the people of the Americas to enjoy a secure cyber environment. The results of this report confirm the need for regional leaders to redouble efforts to support the protection of our various critical national assets.

As a region, we have made great strides and continue to improve effective cooperation in the area of hemispheric security. Our focus now must turn to thinking more strategically about critical infrastructure and critical information protection in the region and to providing the necessary incentives and environment to foster good practices in this area.

FOREWORD

Tom Burt
Vice President and General Counsel for Digital Trust
Microsoft Corporation

Critical infrastructure protection: The time to act is now

Governments around the world are turning their attention to cybersecurity. Their priorities range from increasing cybersecurity skills, to adoption of new cybercrime laws, to understanding how existing or new international rules might apply to the new theatre of cyberwarfare. One commonly identified priority is protection of critical infrastructures – the services, systems and functions upon which modern nations depend – from cyberattack.

The large scale cyberattacks we have witnessed in 2017, WannaCry and NotPetya in particular, brought that reality closer to home. While the world's infrastructures escaped relatively unscathed - allowing for the substantial economic cost incurred by governments and private enterprise around the world - the attacks made the potential impact on our hospitals, ports, telecommunications, energy supply and other government services much more real. In this new era of cyberthreats, protecting and increasing the resilience of critical infrastructures is more important than ever.

This report, in which Microsoft is delighted to have been able to partner with the Organization of American States (OAS) is therefore all the more timely. In the report we: i) examine the threats faced by countries in Latin America and the Caribbean, ii) survey regional cybersecurity, and iii) put forward best practices and suggestions for the road ahead.

The report is the latest in a line of the Microsoft initiatives, often in partnership with others, to encourage governments to develop and embrace a prioritized approach to critical infrastructure protection, grounded in risk management. Among these efforts, we have called for development and adoption of globally harmonized cybersecurity baselines for critical infrastructure. To this end we have partnered with the United States' National Institute of Standards and Technology (NIST) in their development and review of the NIST Cybersecurity Framework and advocated for its adoption as an international standard.

However, we have also come to realization that our calls for increased investment in defensive practices might not be sufficient. We have therefore also proposed a Digital Geneva Convention, asking governments to exercise restraint when it comes to investing in offensive cyber operations and commitments not to attack civilians in times of peace. One of its suggested pillars is that government should not attack critical infrastructures of other nations. I hope that our proposal is heeded, but in any event this report will help increase the resilience of critical infrastructures, not only in Latin America, but around the world.

CRITICAL INFRASTRUCTURE PROTECTION IN LATIN AMERICA AND THE CARIBBEAN 2018

TABLE OF CONTENTS

CRITICAL INFRASTRUCTURE PROTECTION IN LATIN AMERICA AND THE CARIBBEAN 2018

INTRODUCTION

The advances in digital technology have completely revolutionized the way individuals, companies and states interact. The delivery of government services, as well as the overall flow of goods and services, have been transformed because of increased Internet connectivity and the advent of e-trade and e-businesses. Nevertheless, new technologies bring with them challenges and threats of their own.

The adoption of new digital technologies allows for a more efficient management of critical infrastructures in terms of scale, distance, and time, but also introduces new vulnerabilities that make the protection of critical information infrastructures an important, and challenging task. The protection of information assets and systems that support and form critical infrastructures, i.e. the critical information infrastructures (CII), has therefore become a major concern for national security policies as new technologies are adopted. Critical Information Infrastructure Protection (CIIP) can be defined as: "All activities aimed at ensuring the functionality, continuity and integrity of CII to deter, mitigate and neutralize a threat, risk or vulnerability or minimize the impact of an incident".[1]

While critical infrastructures and CII are interrelated and both are crucial for the well-functioning of a society and its security, these concepts cannot be used interchangeably and require different methods of management, control, and protection. While several definitions of critical infrastructure exist, and nations differ on which sectors fall under the classification, commonly critical infrastructures are considered "those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences".[2] Hence, the continuous protection and risk management of those infrastructures are crucial for their resiliency and the security of each nation.[3]

Digital technologies are being increasingly adopted for the management, maintenance, control, and protection of critical infrastructures, for example with industrial control systems (ICS), or used as an infrastructure itself, as with telecommunication services or internet exchange points.[4] These are referred to as CII and commonly defined as "networks of information and communications technologies (ICT) and data that support, link, and enable critical infrastructure operations, and whose disruption, destruction, or exploitation could have a debilitating impact".[5]

This report aims to reflect the experiences and practices of critical infrastructure and critical information infrastructure protection in Latin America and the Caribbean. As a region with a long history of cooperation and one of the first to cooperate on addressing cybersecurity threats, these learnings can be a valuable reference for the cybersecurity and critical infrastructure community as a whole.

1. GFCE (2016). P.6.

2. European Council, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

3. Microsoft (2014), Critical Infrastructure Protection: Concepts and Continuum: www.query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVtZU

4. GFCE (2016), The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers: www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

5. Microsoft (2014). P.4.

The challenges of CII protection

Protection of CII is difficult for several reasons including, but not limited to, the following: (1) the global interconnectedness of information infrastructures; (2) the inability to precisely measure the impact of a cyber-attack; (3) the dispersed responsibility for cybersecurity; and (4) the constantly-evolving cyber-threat landscape.

Global interconnectivity

As with all aspects of our lives, CII are increasingly connected and operating in a world without clear borders, which allows for much freer and less controllable flows of information and data. There are clear benefits to this, particularly in terms of efficiency and productivity. However, this same interconnectedness also makes critical infrastructure vulnerable to cyber-attacks. A particular country's CII can become a target for cyber-attacks, or indeed a means for attacking another nation's CII. In short, a vulnerable CII can become the weakest link in the global network, making CIIP a focal point for universal collaboration and effort.[6]

However, before any partnership can be embarked upon, countries need to recognize that this is an area of policy where it is in everyone's interest, and vital, to cooperate. To do so, nations need to understand their specific national threats and vulnerabilities. A national cybersecurity strategy, and more specifically a national CIP framework, can help with that. It is important to note that such a framework, to be effective, must reflect not only an evolving understanding of the motivations and capabilities of threat actors; but also the potential systemic risks that emerge from the complexities of these systems. Further, activities need to take place to promote trust amongst nations so that, for example, information around threats and incidents targeting CII can be shared more readily.

Ability to evaluate impact and loss

One of the core challenges, at both the organizational and national level, is the inability to precisely measure the impact of a particular cyber-attack. This is difficult even for the most sophisticated corporation, as it needs to take into account issues, such as impact on operations, brand damage, fines, and compensation. However, while at the organizational level the impact is likely to be solely economic, the situation is compounded for policy makers, who might have to assess the social consequences of a particular service not being available.

Moreover, the two stakeholders are motivated by different priorities. At the organizational level, the priority is protecting the entity in question. As a result, most organizations do not understand how their risks or vulnerabilities might interact with others in the system. Conversely, at the national level, policymakers need to assess when aggregated business risks could constitute a national risk and therefore need to understand the linkages between and amongst the different CIIs. For example, the potential national impact from the compromise, damage, or destruction of a single CII may not rise to the level of national consequence until it is considered in the wider context of other incidents occurring and compounding its impact. When aggregated, such vulnerabilities could create a risk to national economic security.

Dispersed responsibility

CIIs are owned and operated by both public and private stakeholders, making their protection by definition a responsibility that spans both sectors. However, the different sectors regard their particular responsibilities in different ways. Governments tend to look at critical infrastructure as a monolithic collection of systems and services,

6. GFCE (2016); Perry, W. J. (2016): Critical Infrastructure in Latin America: Connected, Dependent and Vulnerable. Center for Hemispheric Studies; www.hds.dodlive.mil/files/2016/05/Pub-OP-Saavedra.pdf

compared to the private sector, which looks at core elements within its direct control or its contractual obligations to deliver services. More specifically, governments tend to allocate resources to address their nation's most pressing threats, securing the most significant assets with substantial effort and attention. In contrast, the private sector concentrates on service delivery, innovation and building market share. These differences in approach can be difficult to overcome, and may compound challenges in communication across technical, management and government audiences.

Protecting CIIs therefore requires continuous cooperation and collaboration between government and private sector actors. Public-private partnerships and working groups therefore need to be at the frontline of CII risk assessment, management and protection.[7] It is important that private organizations, especially those that own and manage information infrastructures, understand their role in CIIP.[8] Similarly, governments, which are responsible for national security and creating the necessary procedures for information exchange amongst stakeholders, need to appreciate that the private sector possesses expert knowledge on the topic.[9]

Ever-changing threat landscape

Threats in cyberspace evolve considerably faster than in other fields, such as in international terrorism or threats to conventional military capabilities. While the latter can take years to change, cyber threats do so constantly.[10] In addition, such threats can come from a plethora of differently motivated actors, from cybercriminals after economic gain, to governments conducting espionage or even offensive military operations.

Given the changing external environment, CIIs and countries need to assess their risks frequently and regularly. As mentioned previously, a risk management framework can help ensure that each individual organization is aware of the risk it faces, agrees on its risk tolerance levels, and puts corresponding mitigations in place. It can similarly help at national level, taking into account that tolerance levels may vary from country to country, as well as from situation to situation. For example, a sustained power outage in the wake of a hurricane may be tolerable, but an unexpected cyber-attack that destroys critical components of energy distribution might not be.

It is also important to note that continuous and effective cybersecurity risk management is a complex and resource intensive task. Prioritizing CIIs involves hard trade-offs between the many roles that governments must serve in protecting citizens and providing national security and more dynamic cooperation with industry partners. CIIP requires new tools and frameworks to be able to effectively assess and manage cybersecurity risks, and protect virtual information infrastructures and traditional, and physical infrastructures alike.[11] It is therefore vital that governments first and foremost focus on functions and services that are truly critical, and that a clear process is in place to ensure all assets, systems, networks or data are identified and, when necessary, designated as a "high priority".

7. Perry, W. J. (2016); Microsoft (n.d.).

8. ENISA (2015); Critical Information Infrastructures Protection approaches in EU: www.resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

9. Abele-Wigert, I., & Dunn, M. (2006). International CIIP Handbook Vol. I - An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies. Zurich: Center for Security Studies, ETH Zurich.

10. Assante, M. J. (2009); Infrastructure Protection in the Ancient World: 42nd Hawaii International Conference on System Sciences, Big Island, HI. doi:10.1109/HICSS.2009.260

11. Microsoft (n.d.);A Framework for Critical Information Infrastructure Risk Management: www.query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc7

THREAT LANDSCAPE- REGIONAL TRENDS[12]

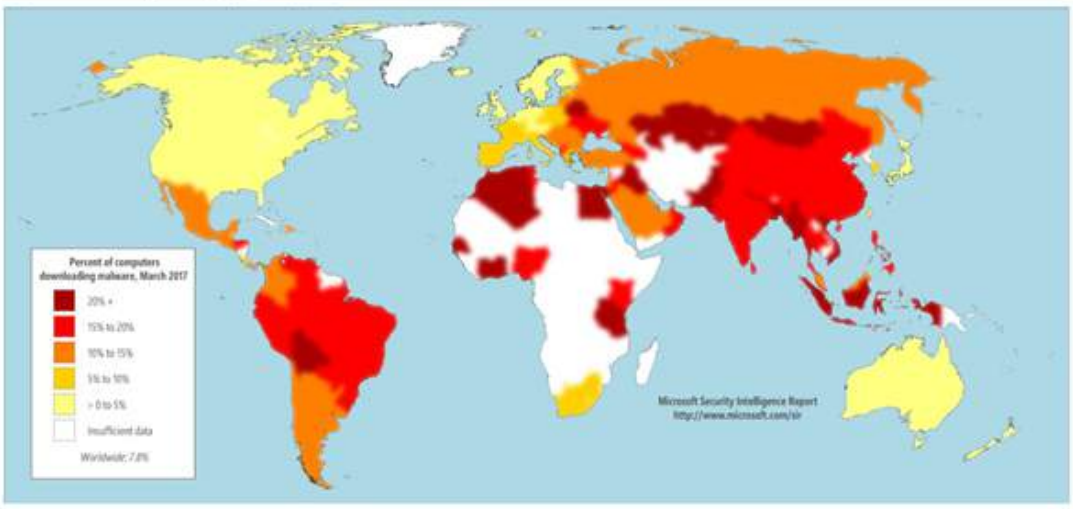
The Microsoft Security Intelligence Report is a bi-annual publication that draws on Microsoft's internal expertise to present the current state of cyber threats. The intelligence that informs it comes from security-related signals from the consumer and commercial on-premises systems and cloud services that Microsoft operates on a global scale. For example, every month 400 billion emails are scanned for phishing and malware, 450 billion authentications are processed, and 18+ billion webpage scans are executed.

This data allows the observation of trends across Microsoft's various platforms, as well as regions. For example, a 300 percent increase in the number of user accounts attacked was observed over the past year. The methodology for account breaches was also noted and therefore recommendations for prevention can be developed. Indeed, a large majority of the compromises just mentioned are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services.

Amongst other findings, the report looks at the percentage of computers running Microsoft real-time security software that report detecting malware or potentially unwanted software, or report detecting a specific threat or family, the so called "encounter rate". For example, the encounter rate for the malware family Win32/ Banload in Brazil in March 2017 was 0.4 percent. This data means that, of the computers in Brazil that were running Microsoft real-time security software in March 2017, 0.4 percent reported encountering the Banload family, and 99.6 percent did not.

The telemetry data generated by Microsoft security products from computers whose administrators or users choose to opt in to provide data to Microsoft includes information about the location of the computer, as determined by IP geolocation. This data makes it possible to compare encounter rates, patterns, and trends in different locations around the world. Using encounter rates, Microsoft learns about the most prevalent threats on both global and per country bases, and uses this information to enhance its security products and services to address those threats.

Encounter rates by country/region, March 2017



12. Microsoft Security Intelligence Report, 2017 https://www.microsoft.com/en-us/security/Intelligence-report

The results for Latin America and the Caribbean by and large continue to be higher than the global average, although there are significant differences between the various countries. Puerto Rico, Canada, and the United States preform particularly well, outperforming the rest of the world, whilst Costa Rica and Panama follow closely.[13]

COUNTRY	JANUARY 2017	FEBRUARY 2017	MARCH 2017
Argentina	13.0%	11.5%	11.1%
Bolivia	19.4%	18.0%	21.1%
Canada	6.0%	5.0%	3.2%
Brazil	19.4%	16.8%	17.0%
Chile	12.0%	10.3%	10.8%
Colombia	15.7%	14.6%	13.3%
Costa Rica	13.0%	11.1%	9.4%
Dominican Republic	17.3%	15.4%	14.9%
Ecuador	18.8%	16.9%	17.9%
El Salvador	15.5%	14.0%	13.7%
Guatemala	15.5%	13.7%	12.8%
Honduras	17.8%	16.4%	16.4%
Jamaica	14.1%	12.3%	12.8%
Mexico	14.1%	12.8%	12.1%
Panama	12.1%	10.5%	10.7%
Paraguay	16.7%	14.6%	15.5%
Peru	18.2%	16.3%	16.9%
Puerto Rico	7.5%	6.4%	6.0%
Trinidad and Tobago	12.1%	9.9%	9.4%
United States	4.7%	4.0%	2.4%
Uruguay	12.2%	11.1%	10.7%
Venezuela	21.4%	18.1%	19.5%
Worldwide	10.3%	9.1%	7.8%

The results of the report make clear that all actors involved in critical infrastructure protection need to take cybersecurity seriously. The following steps are simple actions that help protect your environment:

- Reduce risk of credential compromise by educating users on why they should avoid simple passwords, enforcing multi-factor authentication and applying alternative authentication methods (e.g., gesture or PIN).

- Enforce security policies that control access to sensitive data and limit corporate network access to appropriate users, locations, devices, and operating systems (OS).

- Do not work in public Wi-Fi hotspots where attackers could eavesdrop on your communications, capture logins and passwords, and access your personal data.

- Regularly update your operating systems and other software to ensure the latest patches are installed.

13. Detailed per country analysis is available for Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, Venezuela, and Uruguay: www.microsoft.com/en-us/security/Intelligence-report

GLOBAL BEST PRACTICES FOR CIP

Risk management[14] has emerged as a critical practice in cybersecurity. It typically consists of two sets of practices: one focused on risk assessment (identification, analysis, evaluation of risk), and a second focused on management itself (acceptance, transfer, addressing of risk). The goal of cybersecurity risk management is to move to and maintain an optimal cybersecurity state based on the unique needs, considerations, and best practices of the organization's industry.

> ***With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.***
>
> *NIST Cybersecurity Framework*

Traditionally, risk management relied heavily on the development of "checklists" that can be used by public or private entities to measure compliance. Such an approach to cybersecurity risk management is static in its controls and objectives and rigid in its implementation and does not generally produce results that lead to optimal mitigation of cybersecurity risks, leaving organizations and individuals exposed to attack and exploitation. Instead, risk management needs ensuring that protective measures are implemented based on the integration of threat information, identified vulnerabilities, and a risk reduction strategy. While not a complete solution in and of itself, risk management encourages sound organizational practices that include planning, procedures, budget prioritization, and allocation of key resources (human, monetary, and technical).

A thorough review of relevant literature[15] indicates the following as common best practices to consider in the development of a sustainable CIIP policy or framework.

14. Risk Management is defined as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level (NIST Risk Management Guide for Information Technology Systems - www.csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01)

15. Trend Micro & OAS. (2015) Report on Cybersecurity and Critical Infrastructure in the Americas; ENISA (2015) Critical Information Infrastructures Protection approaches in EU; Brunner, E., & Suter, M. (2009) International CIIP Handbook - An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies. Zurich: Center for Security Studies, ETH Zurich; Dunn, M., & Mauer, V. (2006) International CIIP Handbook 2006 - Analyzing Issues, Challenges, and Prospects. Zurich: Center for Security Studies, ETH Zurich; García Zaballos, A., & Jeun, I. (2016). Best Practices for Critical Information Infrastructure Protection (CIIP) - Experiences from Latin America and the Caribbean and Selected Countries. Inter-American Development Bank (IDB) and Korea Internet & Security Agency (KISA); ENISA. (2014). Incident handling during attack on Critical Information Infrastructure; GFCE. (2016) The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers; Microsoft. (n.d.). A Framework for Critical Information Infrastructure Risk Management (Draft Working Document); National Institute of Standards and Technology. (2017). Framework for Improving Critical Infrastructure Cybersecurity (Draft v1.2); Suter, M. (2007). A Generic National Framework for Critical Information Infrastructure Protection (CIIP). Zurich: Center for Security Studies, ETH Zurich.

GLOBAL BEST PRACTICES FOR CIP

A. Ensure clear division of responsibilities:

Given that CIIP involves multiple stakeholders, with different interests and views regarding CIIP, strong leadership from the government is required to coordinate the multiple agencies that need to be involved in the process of developing a CIIP strategy, as well as in its implementation. The strategy should also clearly determine the various responsibilities for CIIP, across public and private operators, as well as across the different sectors. Timelines and budgets should also be allocated. The 'Generic National Framework for Critical Information Infrastructure Protection'[16], as well as the Organisation for Economic Co-operation and Development (OECD) Council Recommendation on the Protection of Critical Information Infrastructures[17] are helpful guides on achieving that.

B. Engage in a holistic approach:

An effective CIIP policy needs to take a holistic approach that considers technical, economic, organizational, law-enforcement, and security policy aspects and viewpoints. The reason for this is that the operation and protection of CIIP involves a cross section of actors with different roles to play. For example, in the event of a cyber incident, response team may be called in to contain the event, however if the incident is identified as an intentional attack, law enforcement and other security personnel may be called in to investigate. Therefore, the policy should outline clear roles of responsibility and communication channels for all players involved to ensure coordination and a strategic response.

C. Develop frameworks, guidelines and procedures:

Governments should, through an open consultative process, develop clear procedures and guidelines for key processes and aspects of CIIP. The frameworks should be embedded in risk management, whilst still ensuring that CII operators can embrace the latest technology, such as cloud computing, to realize the needed efficiencies. A recommended risk management framework to consider for example includes the NIST Risk Management Framework, which emphasizes that 'the management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for a system---the security controls necessary to protect individuals and the operations and assets of the organization.'

16. Suter, M. (2007). A Generic National Framework for Critical Information Infrastructure Protection (CIIP). Zurich: Center for Security Studies, ETH Zurich

17. Organisation for Economic Co-operation and Development Council Recommendation on the Protection of Critical Information Infrastructures: www.oecd.org/sti/40825404.pdf

GLOBAL BEST PRACTICES FOR CIP

D. Set security baselines:

Security baselines are a foundational set of policies, outcomes, activities, practices, and controls intended to help manage cybersecurity risk. Security baselines are particularly useful in improving cybersecurity because they can cover a range of risks that are typically applicable across a variety of environments. Most risks faced by governments and enterprises are similar, so most "baseline" or fundamental risk management and mitigation activities are also similar. For example, all organizations need to think about regularly reviewing and updating risk assessments, managing how resources are accessed to prevent unauthorized users or behaviors, and planning for and mitigating the impact of incidents.

E. Support dynamic solutions:

Due to the continuous evolution of the cyber landscape, any CIIP solution and approach needs to be dynamic and flexible in nature. Regular and frequent situation and risk reassessments are important to maintain updated solutions and guarantee constant improvements. An example of how to ensure such an approach is the Critical Infrastructure Cyber Community Voluntary Program (C3 – pronounced 'C-Cubed')[18], which was established by the Department of Homeland Security in United States. The C3 Program was established to help critical infrastructure owners and operators use the NIST Framework to manage their cyber risks.

F. Foster trust:

As highlighted above, public-private partnerships between CIIs and the government are essential for CIIP and need to be based on an open exchange of information and expertise. To facilitate such exchange, trust among the parties is essential. The generation of trust can be particularly challenging when partnerships involve competing companies that have a vested interest in keeping their assets and potential security issues from competitors. It is critical that governments help facilitate these exchanges and help protect whole sectors rather than just individual companies.

G. Create projects that demonstrate mutual benefits:

Public-private partnerships, as well as national and international networks, should aim at information exchange and mutual support regarding cyber threats. However, these are difficult to get off the ground. Indeed, for information exchange to be successful in the long-run, its benefits need to be clear to all parties involved. It is therefore important that all participants, whether public or private, share any intelligence and finding they might have to enable security of the group as a whole.

18. Critical Infrastructure Cyber Community Voluntary Program: www.us-cert.gov/ccubedvp

GLOBAL BEST PRACTICES FOR CIP

H. Develop early warning mechanisms:

Early warning systems play a key role in preventing cyber-attacks from spreading, and in minimizing the impact of cyber threats. Thus, both public and private sector should prioritize functions that enable early warning mechanisms. Information exchange between and amongst the different CIIs, as well as with the government, would for example increase the situational awareness of CII operators, enable them to detect a potential attack, and either thwart it or mitigate its impact.

I. Invest in human and technical resources:

CIIP requires employees with particular skills. Identification, recruitment, and retention of cybersecurity experts is crucial to ensuring a high level of security and continuous protection. Moreover, it is important that organizations understand that cybersecurity skills are not a monolith term and that they might need different experts to help them with risk management and traditional IT security, for instance. In addition, organizations should provide regular security training for all staff, as the lack cybersecurity hygiene across the organization is often where entities are most vulnerable.

Furthermore, ensuring that employees are equipped with the necessary technical resources to carry out their jobs effectively is equally important. As a result, sufficient budget allocation for technical cybersecurity products and services is recommended.

J. Improve cyber resilience:

States and enterprises should implement a cyber resilience strategy to ensure business and service continuity in the event of a security incident. It is critical that they go beyond focusing on cybersecurity, but ensure they are prepared for a crisis to occur, be responsive to it, and be able to reinvent its ICT structure in the face of sustained stress and acute disruptions. In other words, being cyber resilient will ensure that businesses or services can continue to be available and operate despite the impact of cyber threats or by natural and man-made disasters.

K. Participate in an international network:

As cyber threats have no physical borders, cooperation across organizations and countries is essential for effective prevention, identification, response, and recovery. Identifying and engaging in existing international structures and frameworks, for example through OAS, the Meridian (see below) or through FIRST[19], can support governmental understanding of the threat environment, as well as keep them in touch with the latest cybersecurity trends and best practices.

19. www.first.org

Part 1

EXPERIENCES AND PRACTICES ADOPTED FOR CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

SURVEY RESULTS
Highlights and Conclusions

CIIs play a central role in modern societies and economies, making their protection an important national and international concern. Their complexity and interconnectedness only amplify the significance of this concern. CIIs are often the aggregate result of functions provided by many owners and operators, technology and service vendors, and governments. The complexity of this value chain, together with the many different stakeholders that ultimately deliver critical infrastructure services, make the security and resiliency of these operations a challenging and shared responsibility.

The understanding of the levels of cooperation between the different entities involved was one of the topics tackled by the survey of Critical Infrastructure Protection (CIP) stakeholders across Latin America and the Caribbean. This survey is the first of its kind for the region and brings to light a number of important findings related to threat perception, as to well as readiness of individual organizations and countries.

The survey results are reproduced in some detail in the section that follows, but it is worth highlighting a number of issues up front. While globally governments have increasingly been working towards adopting cybersecurity frameworks and guidelines to address critical infrastructure protection, this has not been the case in the region. Global initiatives range from strategy development and implementation, information sharing practices, risk assessment and management, to the introduction of security baselines, standards and other technical requirements. **This survey confirmed that the majority of governments across the region have not established incentive programs that could foster the voluntary implementation of cybersecurity measures by CII and CIIP operators and owners or indeed begun to implement mandatory frameworks. We hope that the best practices offered in this publication encourage them to do so.**

However, despite the lack of official frameworks, the survey results indicate **that communication and collaboration exists between the private sector and government**. Indeed, 69% of respondents indicated they participated in working groups, 64% indicated that informal dialogue and/or cooperation takes place, and 42% highlighted the existence of public-private partnerships. These responses reflect established partnerships and practices within the region, which have emerged organically.

Effective CIIP requires employees with a particular skill set and the supporting technology for its protection. Identification, recruitment, and retention of cyber experts is crucial to ensure a high level of security and continuous protection. **Based on the results of the study, 53% of the organizations that responded indicated they had the ability to detect and record cyber incidents. Further, 73% indicated that they had detected a cyber-attack over the last 12 months.**

Respondents to the survey also highlighted good practices. **48% of respondents indicated that they had cybersecurity awareness trainings for employees, 46% indicated they had a disaster recovery plan, 42% indicated they had a cyber incident response plan, 41% indicated they had a documented cybersecurity strategy**. In terms of cybersecurity measures employed by their organization, 82% responded "boundary firewalls" and "internet gateways," 68% indicated "access control," 61% stated "malware protection," 55% "audits" and 50% stated "automated backup." **In regards to risk management, 55% of those that responded to that question indicated that their organization implemented cybersecurity risk management practices and 49% of the respondents indicated they were planning to conduct a risk assessment**. Additionally, 62% of the respondents indicated that there is a dedicated role within their organization to responsible for cybersecurity.

Nevertheless, when asked if there was a dedicated budget for cybersecurity measures, **57% of those that responded indicated they did not have a dedicated budget for cybersecurity measures**. The absence of a dedicated budget often limits the ability of an organization to invest in the resources it needs (i.e. both human and technical) to effectively respond to cyber threats. However, among the ones that had a dedicated budget, a positive result was when asked if their budgets increased over the last year, 59% of those that responded indicated it had.

Despite those positive developments, 69% of the respondents indicated they have noticed an increase in the number of attacks to their computer systems and/or networks over the last 12 months. Additionally, **in terms of the assets that have been the target of the cyber-attacks over the last 12 months, 61% of the respondents identified "data," 58% "company network perimeter," 18% "personnel systems" and 13% indicated "intellectual property."** In relation to the specific attack methods, **76% of those who responded indicated "phishing," followed by 71% identifying "malware" (e.g. viruses, worms, Trojans)**. Other activities identified included port sniffing (no actual intrusion) and social engineering. Interestingly, some identified ransomware and (Distributed) Denial of Service attacks, which when one considers CIIs, are both critical threats for consideration in risk and incident response management.

In conclusion, the report shows that both owners and operators of critical infrastructures in Latin America and the Caribbean have been implementing cybersecurity measures to respond to the evolving threat landscape. And it is positive and encouraging to see the industry respond to threats in a responsible manner. Yet, it is also apparent is that more still needs to be done at the national level across the region. Governments must be more fully prepared given the growing connectedness of their essential services and develop, promote, and implement incentives, best practices, and any necessary regulations to ensure higher levels of security in this space.

Profile of respondents [20]

When asked, 15% of the respondents indicated they were critical infrastructure operators/owners, 60% identified as critical information infrastructure operators/owners, and 25% answered "other". The last category, 'other,' included national regulators, cyber defense command, Internet Service Providers (ISP), and computer security incident response teams. For the purposes of this question, critical Infrastructure was defined as systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matter.

60% of the respondents identified as critical information infrastructure operator/owner

Similarly, the industries represented covered a wide spectrum of sectors. Out of the 497 respondents, 29% were from central government, 19% from telecommunications/ICT, 9% from banking and finance, and 7% represented military defense/army/defense facilities. Additional respondents came from the energy/electricity (chemical, nuclear, gas, oil, other), and transportation (air, sea, land)/logistics/distribution sectors, among others.

20. In the development of this report, a survey was conducted to help inform our findings. 881 persons attempted the survey, with 11% of respondents from the Caribbean and 89% from Latin America and an average completion rate of 341 respondents.

When it comes to the type of systems operated by the respondents, when asked 'Do you have a Supervisory Control and Data Acquisition (SCADA/ICS) system?', which comprises systems that are used to monitor and control industrial processes, of the respondents to this question 80% responded they did not.

WHICH INDUSTRY DO YOU BELONG TO?

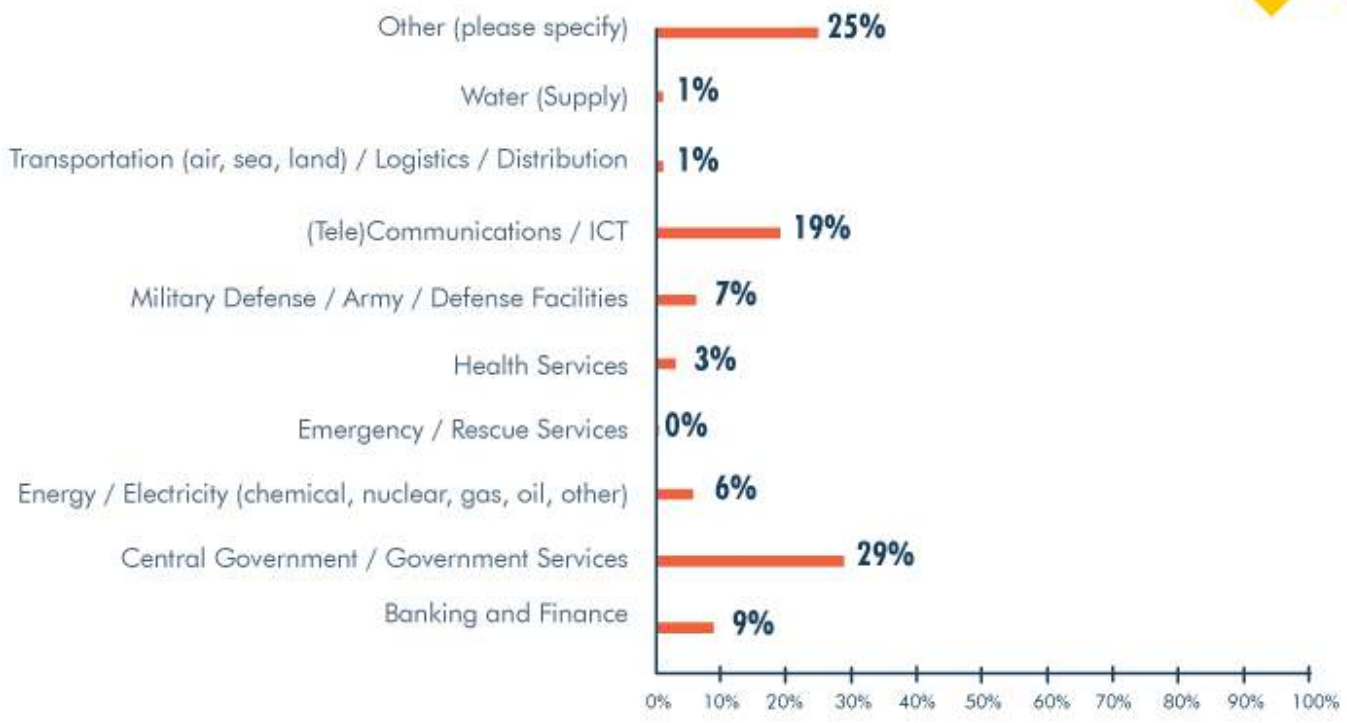


Figure 1 Total respondents, n= 497

In terms of the size, 42% of the respondents indicated they had 1-500 employees, while 58% indicated they had 500+.[21]

21. Total respondents, n=462

Ability to detect cyber incidents

An effective incident response plan depends on three core capabilities: being able to protect, detect, and respond to threats. Protection is about preventing incidents, detection is about identifying threats early, and response is about evicting the attacker and restoring systems to mitigate the impacts of a breach. The ability to detect an attack on the network is particularly important, as the earlier an incident is detected the sooner measures can be put in place to reduce the impact of the incident. It is important to zzote that surveys analyzing the length of time it takes to detect an attack, again and again find that detection does not usually occur in minutes or hours, but often times are identified months after the first intrusion.

Detection can be even more difficult for CIIs. They are often required to be operational at all times, making regular patching and upgrades difficult, and irregular emergency updates near impossible. That can make them more vulnerable, and therefore, integrated detection and intrusion software that supports early detection, as well as having well-trained personnel, is crucial.

When asked whether their organization had the ability to detect cyber incidents, 53% of respondents indicated that they had detection capabilities in place and were monitoring how often cyber incidents occurred. In comparison, 11% believed their organization did not have any detection measures in place or indeed any plans to implement them. 35% of the respondents were planning to invest in appropriate tools to enable incident detection.

The results were similar across the Caribbean and Latin America, with 59% of the respondents from the Caribbean and 53% of the respondents from Latin America indicating they had detection capabilities; and 27% of the Caribbean and 36% of Latin American respondents indicating they are planning to invest in the implementation of detection measures.

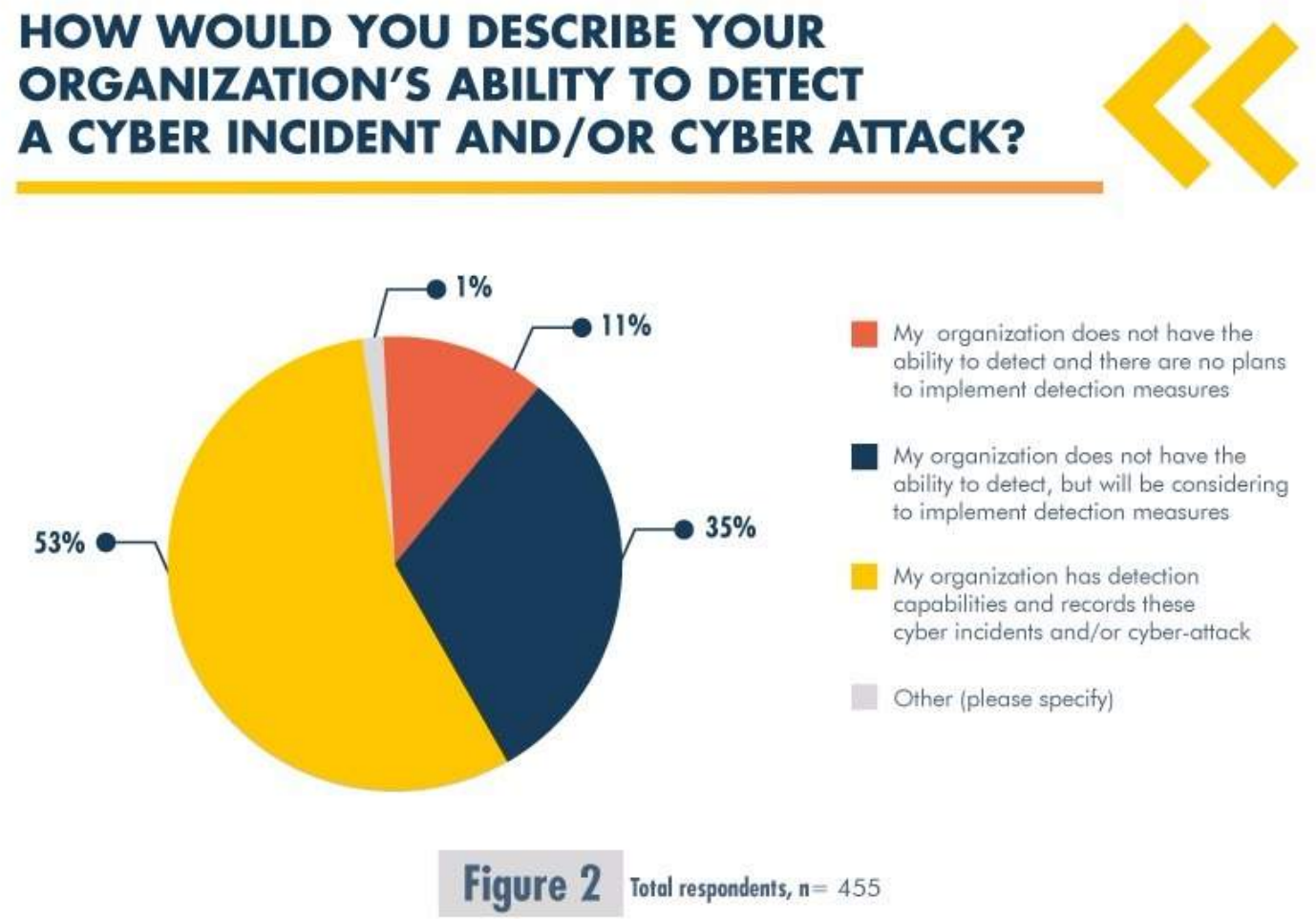


Figure 2 Total respondents, n= 455

As a follow up question, the respondents were asked whether they have detected attacks against their organization's computer systems or networks in the past 12 months. 73% of the respondents answered in the affirmative.[22]

Figure 3 Total respondents, n= 453

Frequency of cyber incidents

According to the 2018 World Economic Forum Global Risks Report[23], cyber-attacks are among the top global risks, alongside extreme weather events, natural disasters, data fraud or theft, and failure of climate-change mitigation and adaptation. Irrespective of which survey or report you pick up, the frequency of cyber incidents seems to be increasing, and dramatically so. Microsoft's 2017 Security Intelligence Report[24] showed a 300% increase in attacks on cloud platforms, whilst other surveys showed similar triple digit growth in ransomware or other attacks.

Our survey showed similar results. In responding to whether the organizations have detected an increase in the number of attacks on their computer systems and/or networks, almost 69% of the respondents indicated that they noticed an increase, with only 22 % indicating no change, and only 9% indicating they have noticed a decrease. These results show that investing in cybersecurity is more important than ever.

22. Total respondents, n= 453

23. World Economic Forum Global Risk Report, 2018: www.reports.weforum.org/global-risks-2018/

24. Microsoft Security Intelligence Report, 2017: www.download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf.

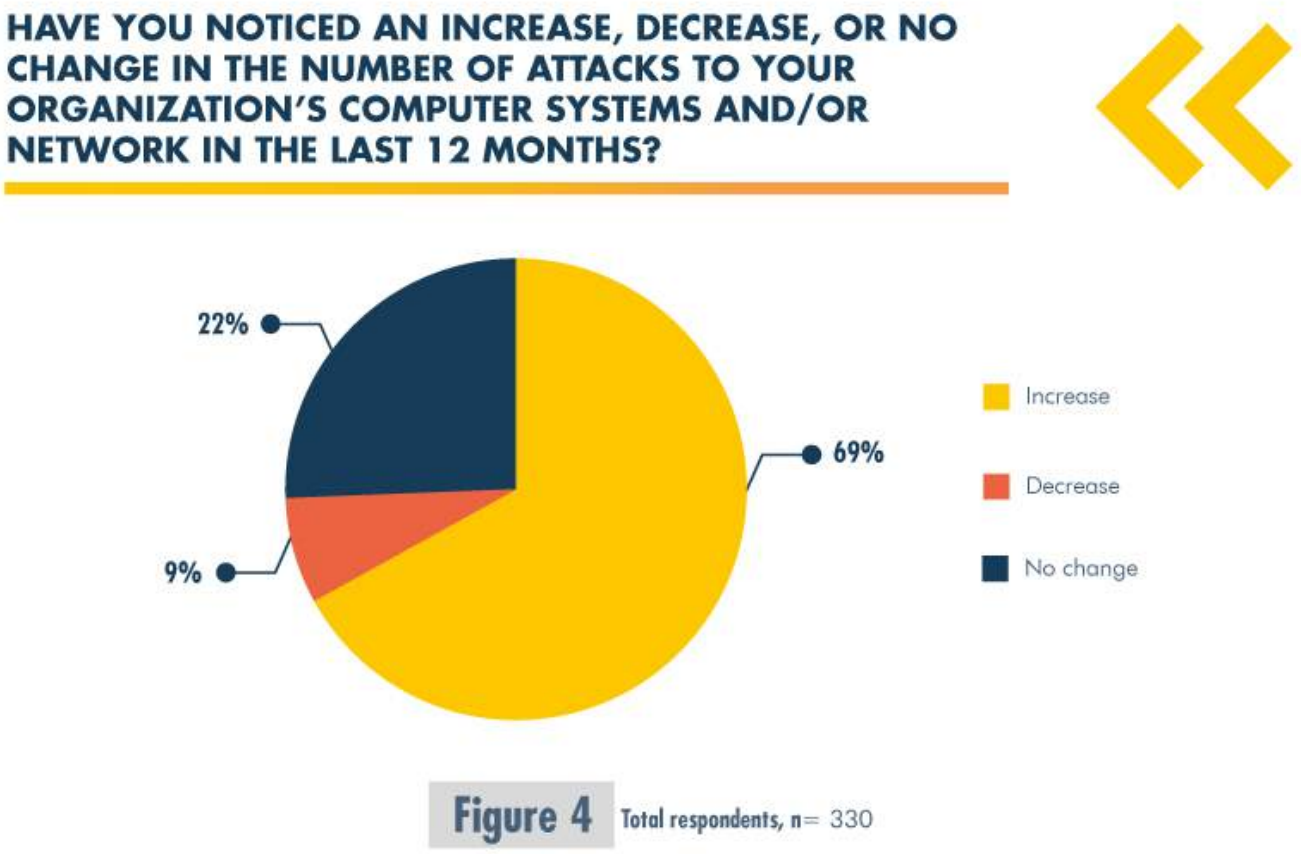


Figure 4 Total respondents, n= 330

Types and methods of cyber-incidents

CIIs can be particularly attractive targets for a whole range of malicious actors, from criminals to other nations. This is not only because they contain valuable information and data, but also because their operations are critical to national security. Therefore, malicious actors might target them not with intent to steal, but with intent to sabotage their operations. In 2017, for example, a security vendor[25] identified a cyber-attack based campaign, now referred to as Dragonfly 2.0, which targeted energy facilities in Europe and North America. The Dragonfly group appears to be interested in both learning how energy facilities operate and also gaining access to operational systems themselves, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so.

The risks to CIIs can therefore be greater and more complex than would be the case with any other private sector entity. The likelihood of sophisticated actors targeting them is greater, given the vital role they play in society. In addition to threats we have already highlighted, as global terrorism continues to evolve and as these groups gain greater capabilities online, they are also likely to focus on where they could have the greatest adverse impact on national economies and security - CIIs are likely to be amongst their primary targets.

Whilst our survey did not seek to attribute the attacks to particular actors, we have sought to determine where the majority of cyber-incidents originated from. Respondents were asked what type of incident they have experienced in the past 12 months, with the options given including insider threats, force majeure, technical failure, and cyber-attack. The vast majority of respondents (54%) highlighted external attacks on their cyber assets, 24% indicated that technical failure was to blame for the incident, 18% blamed internal cybersecurity incidents, and 11 % called out force majeure.

25. Symantec, Dragonfly: Western energy sector targeted by sophisticated attack group www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

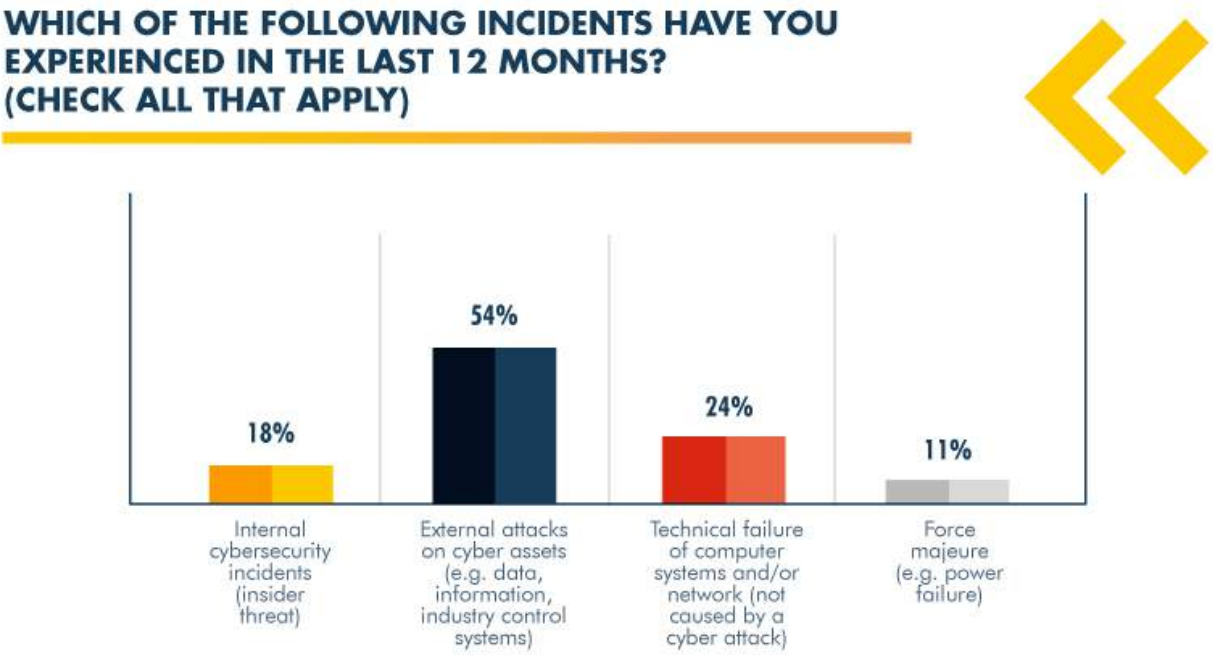


Figure 5 Total respondents, n= 317

When asked what methods were used in the attack, 76% of the respondents indicated phishing, and 71% various malware attacks. Other methods observed included port sniffing (no actual intrusion) and social engineering. 46% identified ransomware and 36% (Distributed) Denial of Service attacks. While phishing in particular can be associated with sophisticated and persistent attacks, the last two are particularly important to mention in the context of CII, as they are likely to result in a series disruption of service.

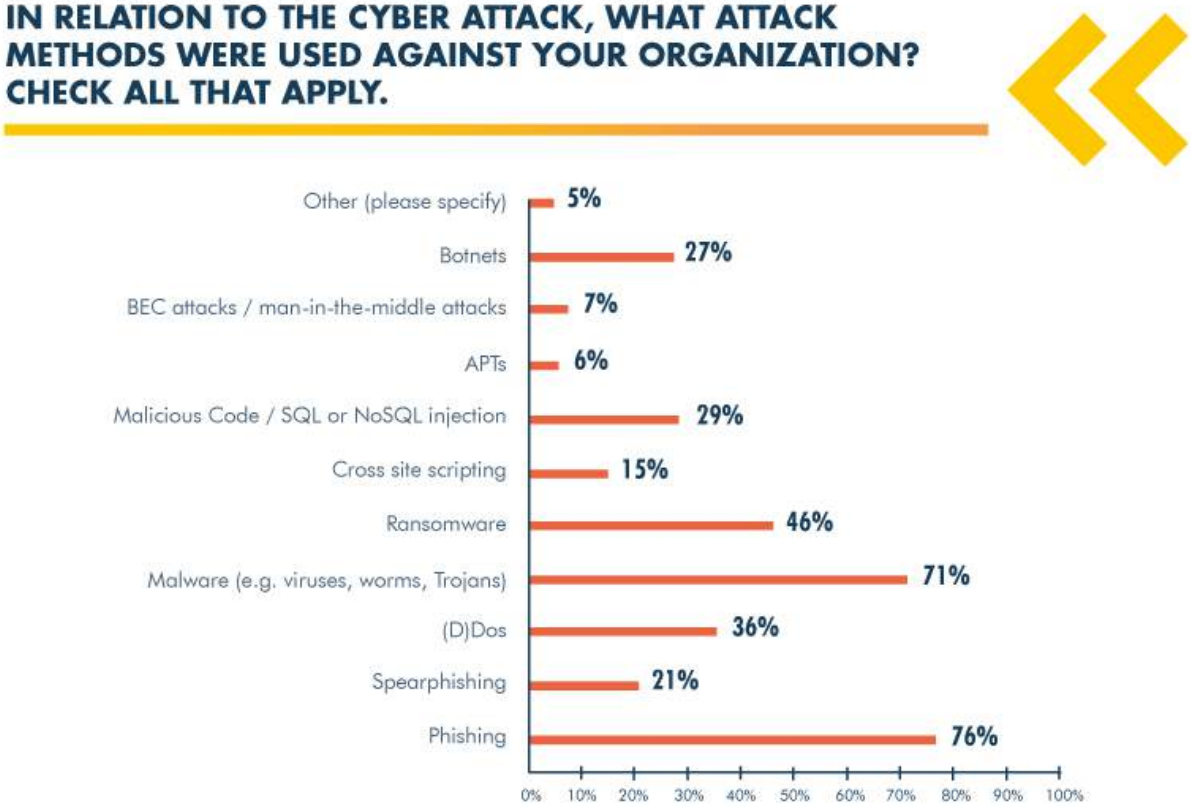


Figure 6 Total respondents, n= 311

Sophistication of cyberattacks

A sophisticated cyberattack will employ a variety of effective tools and tactics: phishing scams, malware and spyware attacks, browser and software exploits, access through lost and stolen devices, and social engineering. Traditional security tools have largely focused on prevention. However, the sophistication and scale of advanced persistent threats (APTs) means that while preventing a breach is ideal, and a critical part of operations, it is not realistic to focus exclusively on protection. Organizations need to recognize that breaches are hard to detect and assume that a breach has already occurred.

Indeed, when the respondents were asked whether cyber-attacks on their systems were getting more sophisticated, 62% of the respondents indicated 'Yes', with 30% indicating they were unsure. A possible explanation as to why the respondents may be unsure of the level of sophistication is that globally some of these attacks are become increasingly difficult to detect. Moreover, many might not have the tools and capabilities to measure progress over time, given the fairly large proportion of respondents that have at the onset indicated they have limited detection capabilities in place. As stated above, tracing an incident often requires the right technical and human resources and, even then, detection is not guaranteed.

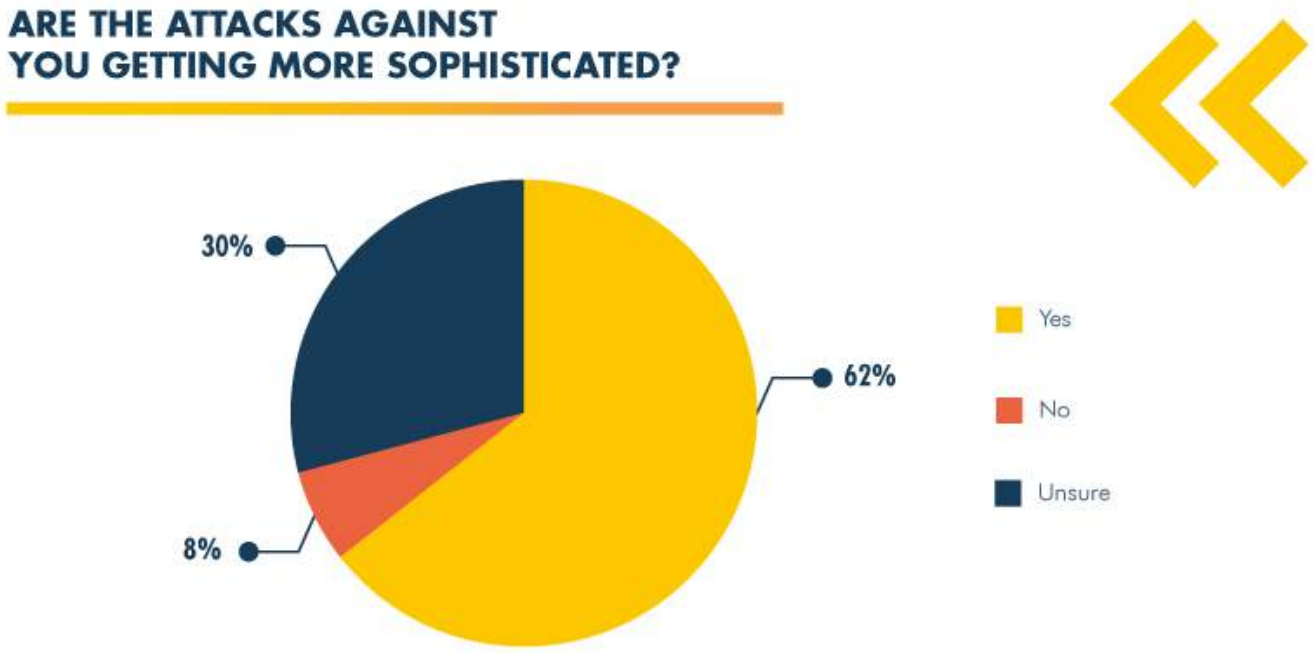


Figure 7 Total respondents, n= 320

Impact of cyber incidents

As a core principle of cybersecurity risk management, an organization should not only be able to detect cyber incidents, but also have the capability of assessing their potential impact ahead of time and thus be able to prioritize assets that are most critical. Similarly, it is important that organizations identify, analyze and learn from intrusions that occur. This approach will ensure they are able to avoid making the same mistakes in the future, making their organization more resilient in the process.

In response to the question, 'What happened to your organization as a result of the attacks experienced?', 44% of the respondents indicated that nothing happened, while 33% indicated that they experienced some business interruption (downtime). 22% of the respondents indicated that the attackers were able to gain

unauthorized access to and/or theft of classified or sensitive information, and 17% indicated that there was some modification, destruction or deletion of data or information. Other areas identified included damage to reputation and data hijacking.

Figure 8 Total respondents, n= 303

Cause of intrusion

Understanding what led to the incident occurring is critical to the ability of the organization to learn from the past and increase its cyber resilience. In answer to the question, 'What are the top 5 causes that the attack(s) could have resulted from?', the top 5 causes in order of highest ranking were:

1. Lack of cybersecurity awareness among employees
2. Lack of security skills
3. Poor/inadequate patch management
4. Inadequate access controls
5. Lack of budget to support application security initiatives and Issues within application of security within the organization both tied at 5th.

The other areas identified included insecure code development, poor/inadequate testing methodologies and poor deployment and configuration.[26] These findings are in line with many such surveys, including the Microsoft Intelligence Security Report referenced above, and underline the need for basic cybersecurity hygiene across the organizations. In addition, many best practices highlight patch management and access controls as vital to securing any entity, indeed some have claimed that implementing those can reduce cyber-attacks up to 90%. The UK's Cybersecurity essentials scheme[27], for example, highlights those two best practices, but also securing the Internet connection, devices and software and implementing antivirus software. Similarly, they highlight the importance of dedicating specific resources, both human and monetary and technical, to cybersecurity, ensuring that it remains a continuous priority.

26. An example of cybersecurity measures is the Water ISAC 2015 10 Basic Cybersecurity Measures, Accessed at: www.ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

27. Cybersecurity essentials: www.cyberessentials.ncsc.gov.uk

FROM THE LIST BELOW, WHICH ARE THE TOP 5 CAUSES THAT THE ATTACK(S) COULD HAVE RESULTED FROM?

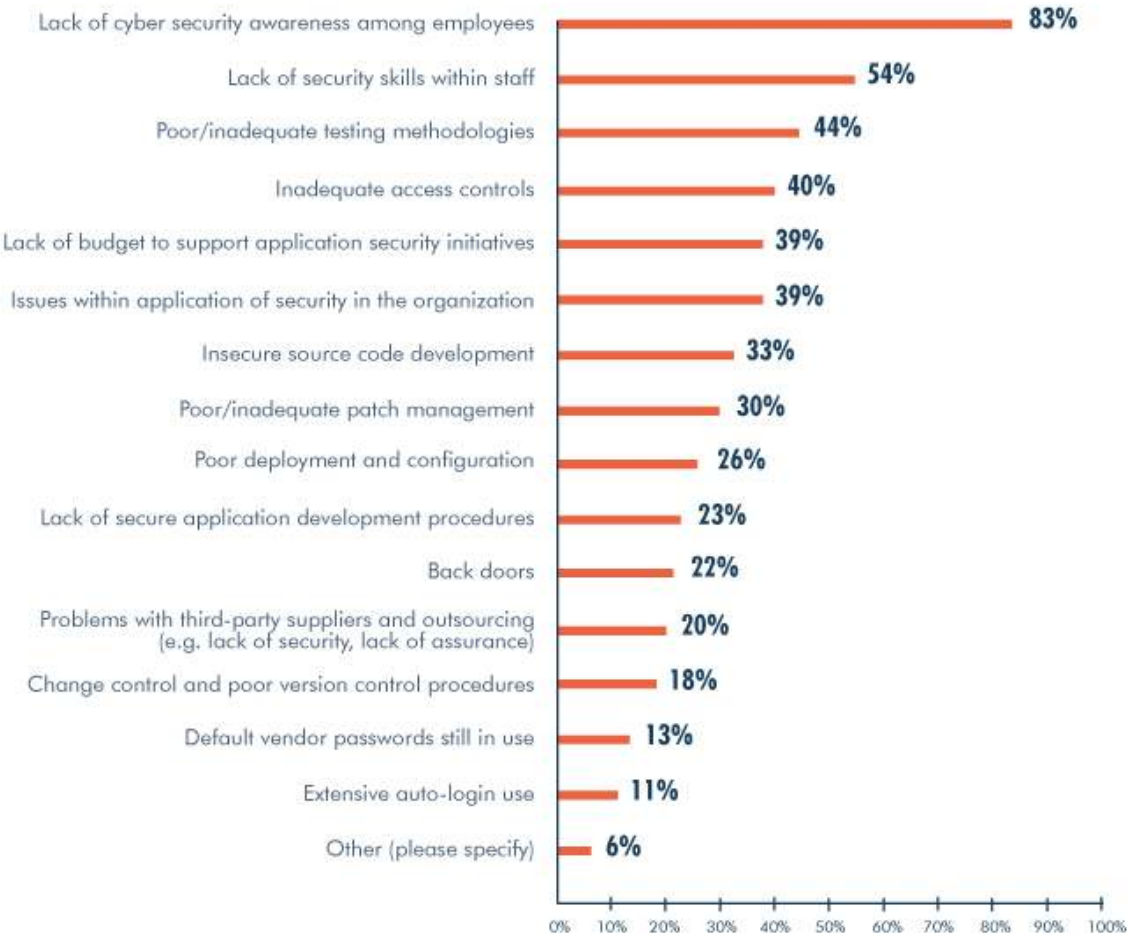


Figure 9 Total respondents, n= 288

Understanding the organization's assets

A further important component of cybersecurity risk management, is the need for a clear understanding of the motivations and capabilities of threat actors, potential avenues for attack or exploitation, as well as the key assets, functions or information that could be targeted. A clear analysis and understanding of threats, as well as risks and vulnerabilities, is essential for an organization to be able to prioritize the allocation of budgetary and other resources necessary for its protection.

When asked 'Which cyber assets has your organization identified as critical?.', 89% of the respondents identified data as critical, 57% highlighted the company network perimeter, and 41% personnel systems. Building on the previous question, when asked which asset was the target of a cyber-attack in the last 12 months, 61% of the respondents identified data, 58% the company network perimeter, 18% personnel systems, and 13% intellectual property. These results are helpful as they can indicate what type of information the attackers were after, highlight the most vulnerable organizational assets and form a basis for the development of a risk management framework.

WHICH CYBER ASSETS HAS YOUR ORGANIZATION IDENTIFIED AS CRITICAL? CHECK ALL THAT APPLY.

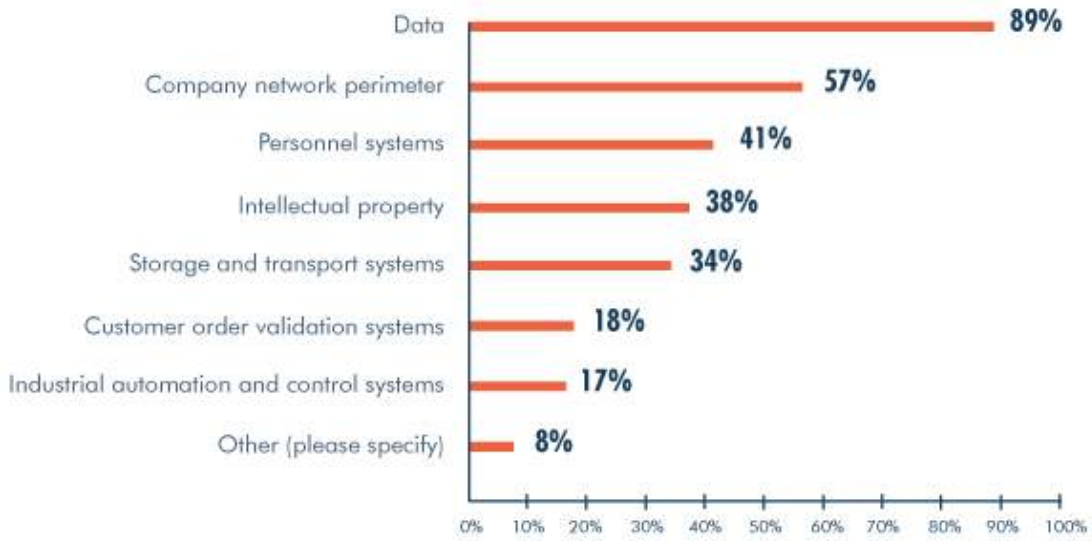


Figure 10 Total respondents, n= 321

WHICH ONE OF THE FOLLOWING ASSETS OF YOUR ORGANIZATION HAS BEEN A TARGET OF A CYBER ATTACK IN THE LAST 12 MONTHS? CHECK ALL THAT APPLY

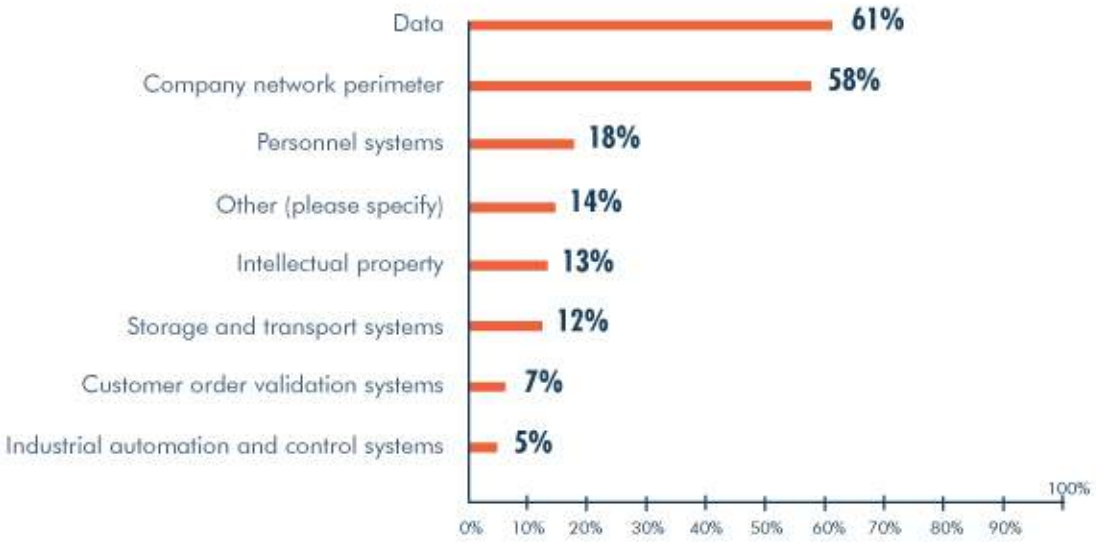


Figure 11 Total respondents, n= 360

Cybersecurity measures

Earlier in the survey we focused on incident detection; however other measures are just as important for improving cybersecurity of organizations. Numerous organizations have put forward examples of what these could be, the most frequent being: secure your Internet connection, secure your devices and software, control access to your data and services, protect from viruses and other malware, and keep your devices and software up to date.[28]

When asked 'What sort of technical cybersecurity measures does your organization have in place in relation to Critical Infrastructure Information (CII) systems?, the majority of respondents highlighted boundary firewalls and internet gateways (82%). Other measures included access control (68%), malware protection (61%), audits (55%), and automated backup (50%).

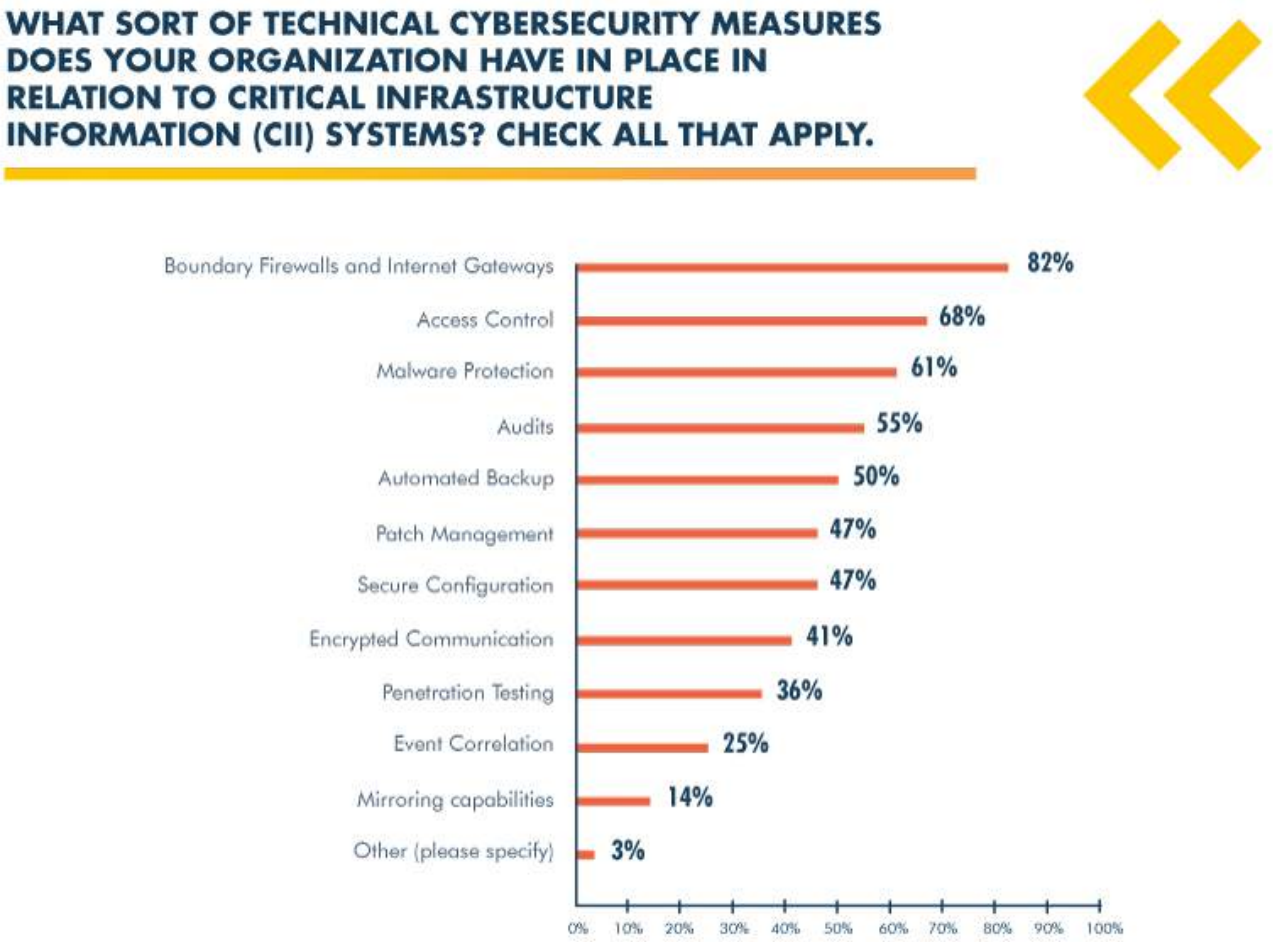


Figure 12 Total respondents, n= 404

As stated earlier in the report, having clear frameworks, guidelines and procedures are key considerations for the development of a sustainable CIIP policy. When asked, 'Does your organization have cybersecurity policies/ and or plans?', some of the highlights were that 48% of the respondents indicated that they had cybersecurity awareness training for employees in place, 46% indicated they had a disaster recovery plan, 42% indicated they had a cyber incident response plan, and 41% indicated they had a documented cybersecurity strategy.

28. An example of this is Cyber Essentials UK, www.cyberessentials.ncsc.gov.uk/ or UK government's 10 steps to cybersecurityhttps://www.ncsc.gov.uk/guidance/10-steps-cyber-security

DOES YOUR ORGANIZATION HAVE CYBERSECURITY POLICIES AND/OR PLANS?

Figure 13 Total respondents, n= 392

When asked to identify the 'recognized standards or frameworks' their organization uses to assess and mitigate cyber risk, the respondents most frequently identified included COBIT[29], ISO[30], IEEE[31], IEC[32], ITIL[33], OWASP[34], SANs[35] and NIST, referenced elsewhere in the document.

In response to whether they have a dedicated role to address cybersecurity, the majority of the respondents indicated 'yes' (62%), with only 38% indicated 'no'. Further, when asked what level supervises cybersecurity efforts within their organization, 42% indicated their IT department and 19% the information security department, with only 13% identifying the C-Suite. Interestingly, only 4% indicated that this role was outsourced to an external consultant/contractor. This reality however, forces one to consider at what level cybersecurity issues should be dealt with. For example, allocating this task to IT alone, isolates other key areas within an organization that should be involved in the risk management of its operations. Conversely, the traditional risk management departments might not have the skills required.

29. Control Objectives for Information and Related Technologies (COBIT): www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf

30. International standards organisation (ISO): www.iso.org

31. Institute of Electrical and Electronics Engineers: www.theinstitute.ieee.org/technology-topics/cybersecurity/ieee-standards-on-cybersecurity

32. International Electrotechnical Commission: www.iec.ch/about/activities/standards.htm

33. Information Technology Infrastructure Library: www.bmc.com/guides/itil-information-security-management.html

34. Open Web Application Security Project: www.owasp.org/

35. www.sans.org

WHAT LEVEL SUPERVISES CYBERSECURITY EFFORTS AT YOUR ORGANIZATION?

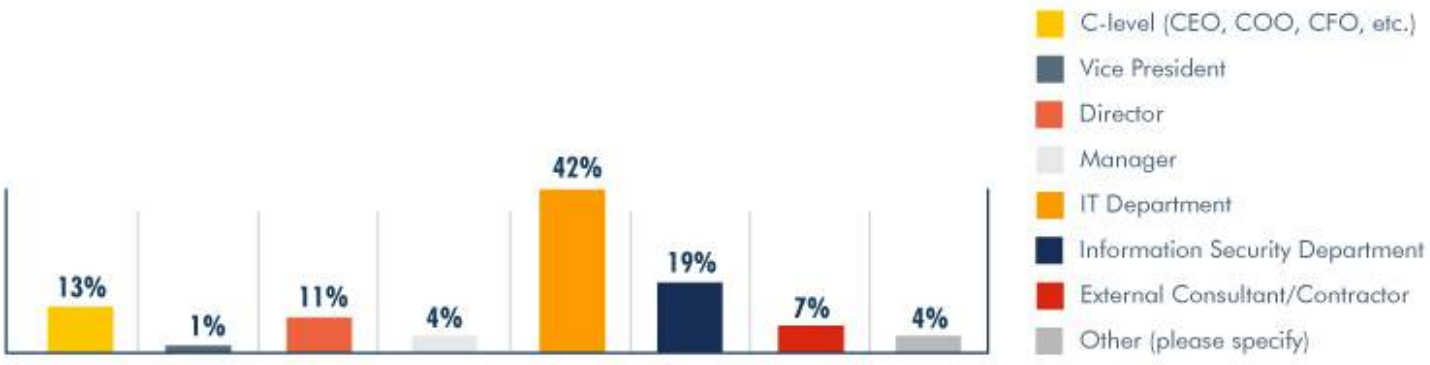


Figure 14 Total respondents, n= 366

Dedicated budgets

Risk management guidance consistently highlights the importance of communication across organizations, both horizontally and vertically. However, cybersecurity risk management is a relatively new and technical topic for many company managers, directors, and boards, so they may struggle with cross-organizational and vertical engagement on the issue. Bridging cybersecurity risk management understanding across audiences by using common language enables stakeholders to communicate in a meaningful way about the risk landscape, resulting in more informed decisions about how to prioritize and manage risks, and creating continuity in security strategy, planning, and investments. If executives can understand what practitioners are aiming to achieve and regularly revisit progress on a relatively consistent set of desired security outcomes, then they may better understand the strategic value of resourcing practitioners to meet goals or to address gaps.

When the respondents were asked if there was a dedicated budget for cybersecurity measures, 57% of those that responded indicated 'No'. The absence of a dedicated budget often limits the ability of an organization to invest in the resources it needs (i.e. both human and technical) to effectively respond to cyber threats.

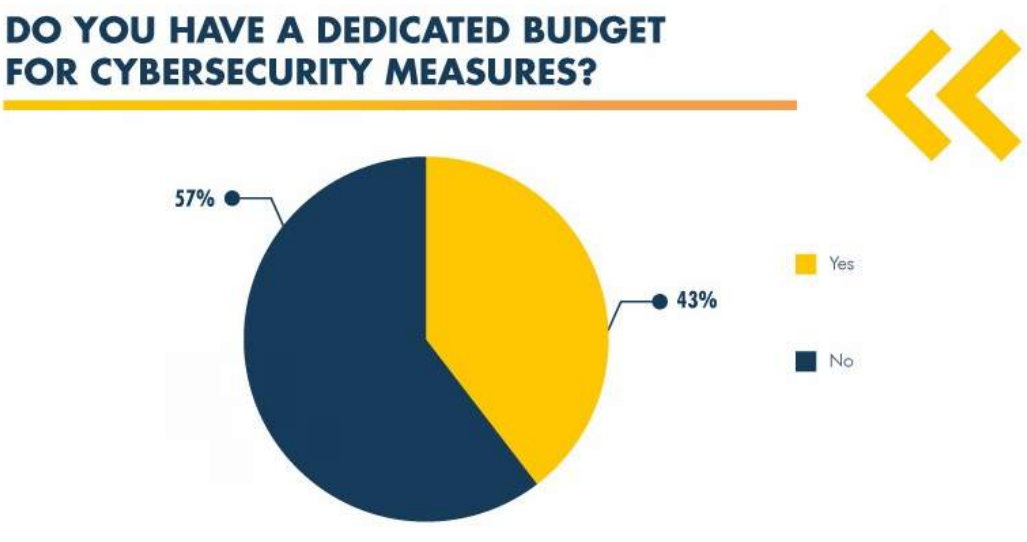


Figure 15 Total respondents, n= 359

Comparatively, however, when asked if their budget for cybersecurity has increased over the last year, 59% of those that responded indicated that it had increased. As a follow up, the respondents were then asked 'Does your organization measure effectiveness of your cybersecurity budget?', 57% of those that responded indicated that they do. This is a positive result from the analysis as it demonstrates that the respondents not only allocate for cybersecurity measures, but evaluate the effectiveness and make adjustments accordingly (for example, the ones who saw a positive increase in the last 12 months).

Risk management

Many measures, such as the ones identified above, are geared towards mitigation of risks and ensuring the resilience of critical infrastructure. Risk management, for the purpose of this survey, involves the identification, analysis, and assessment of potential hazards in a system or hazards related to a cybersecurity on an on-going basis with the aim of identifying tolerable risks and implementing mitigation measures to either eliminate or reduce the risk potential. However, while individual parts of implementing risk management initiatives might be under way, a much smaller number of organizations in this survey have taken a comprehensive approach.

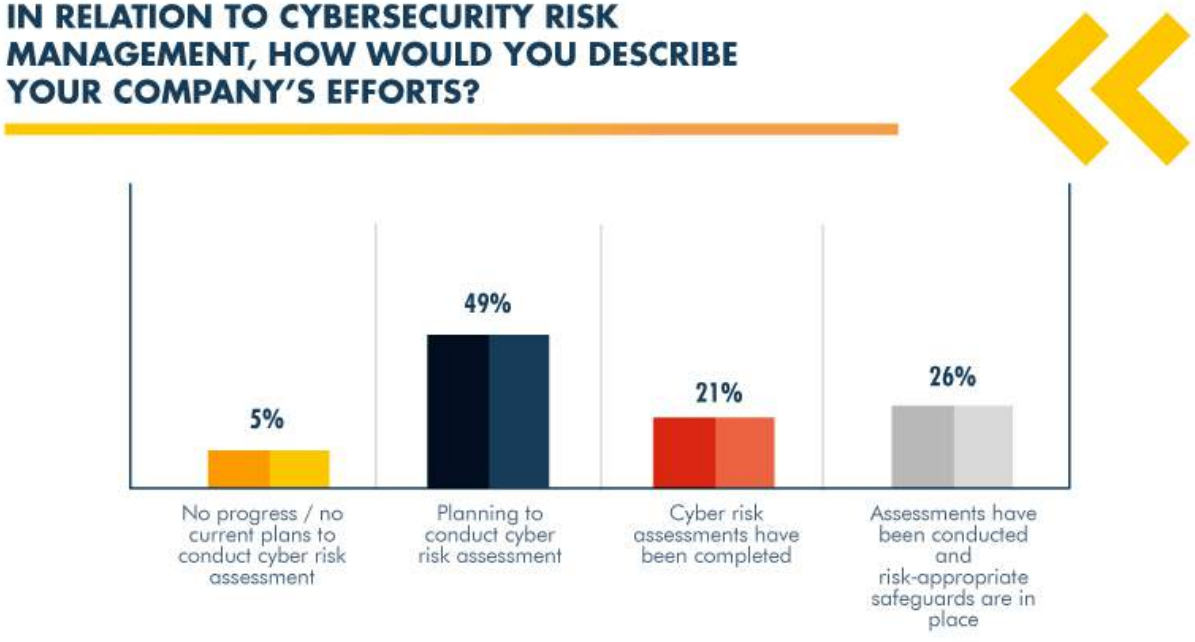


Figure 16 Total respondents, n= 222

When asked, 'Does your organization implement cybersecurity risk management practices?', 55% of the respondents indicated 'yes' and 45% responded 'no'. However, in the follow up question 'In relation to cybersecurity risk management, how would you describe your company's efforts?', the responses were more encouraging, 49% of the respondents indicated they were planning to conduct a risk assessment, 26% indicated assessments had been conducted and risk appropriate safeguards were in place, 21% indicated that cyber assessments had been completed and only 5% of the respondents indicated that no progress/no current plans were in place to conduct a cyber risk assessment.

Figure 17 Total respondents, n= 402

Coordination at national level

Governments approach critical infrastructure, cyber threats, and risk assessments very differently than the private sector. In the extreme, policymakers look at critical infrastructure as comprised of monolithic systems and services, while the private sector looks at core elements within its direct control and its contractual obligations to deliver services. Unsurprisingly, governments understand threats to critical infrastructure through the lens of high-end scenarios that could compromise the posture or readiness of national security capabilities and assets that are needed for stability and force projection.

Designated leadership within government is often required to successfully coordinate multiple agencies in the process of developing a CII strategy. However, in response to the question, Does your country have a government agency with responsibility for Critical Information Infrastructure Protection?, only 49% of the respondents from the region answered 'yes[36]'. According to the respondents, the responsibilities assigned to this agency varied, with the most identified role being the issuance of guidelines and recommendations (69%), followed by point of contact for information sharing (56%).

36. Total respondents, n=356

WHAT ARE ITS RESPONSIBILITIES? CHECK ALL THAT APPLY.

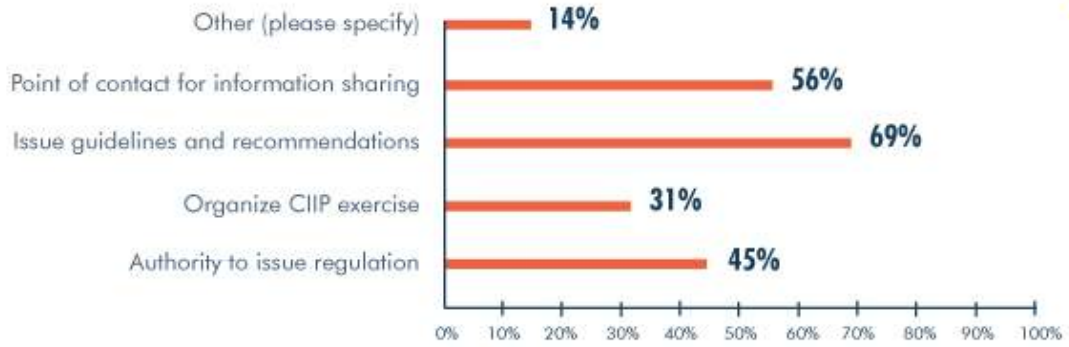


Figure 18 Total respondents, n= 175

Keeping in mind that a majority of the respondents to the question above identified the role of the national agency as being the point of contact for information, when asked 'Is there a discussion/dialogue/cooperation between the government and private sector about the cyber resilience of Critical (Information) Infrastructure systems?', 32% of the respondents indicated they were unsure, 31% indicated 'yes, and our organization participates', 20% indicated yes, but their organization does not participate, and 16% responded no.

Additionally, when asked, 'What kind of cooperation mechanisms exist?', 69% indicated working groups, 64% indicated informal dialogue and/or cooperation, 42% indicated public-private partnerships and only 3% indicated other. This is indicative of good practices within the region in this regard, as the protection of critical infrastructure requires successful information exchange practices which well to the benefit all stakeholders involved.

WHAT KIND OF COOPERATION MECHANISMS EXIST? CHECK ALL THAT APPLY.

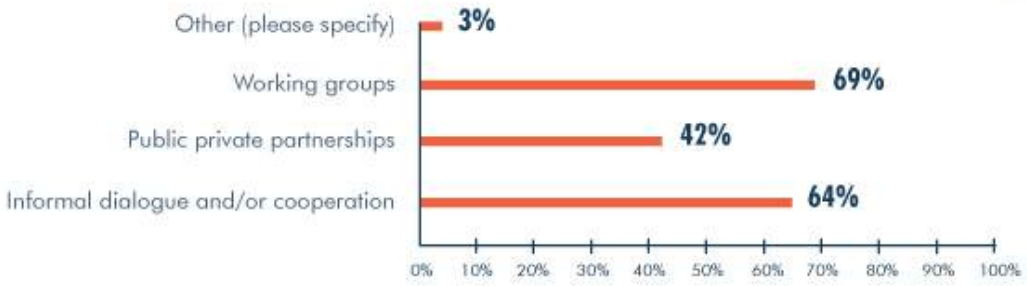


Figure 19 Total respondents, n= 180

In terms of good practices at the national level, when asked if there are any incentives for the CIIs to implement security measures, 78% of those that responded indicated there were no incentives in place, 13% indicated there were official guidelines in place, and only 8% indicated there were financial incentives. As a follow up, when asked, 'Does your country have sector specific regulation related to Critical Information Infrastructure Protection?' 61%[37] of the respondents indicated 'no'. Additionally, when asked if there were any (voluntary) certification framework with regards to cybersecurity in use in your sector and your country, 57%[38] of those that responded indicated 'no'. Finally, when asked if there were any cybersecurity exercises in their country or sector, a majority of the respondents indicated 'no', with only 24% indicating 'yes, and we participate' and 27% indicating 'yes, but we do not participate'.

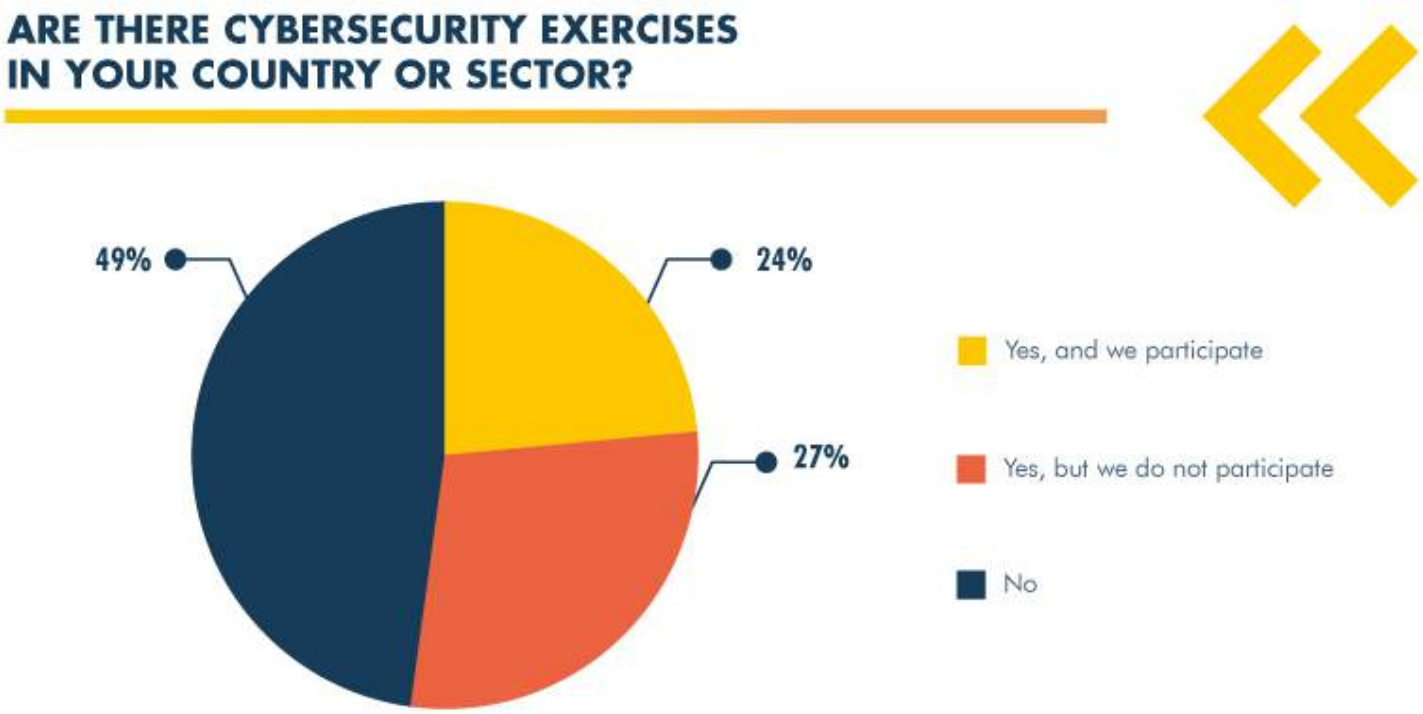


Figure 20 Total respondents, n= 345

37. Total respondents, n=352

38. Total respondents, n=349

Part 2

EXPERIENCES AND GOOD PRACTICES-CASE STUDIES

EXPERIENCES AND GOOD PRACTICES-CASE STUDIES

Lessons learned from the development and implementation of information technology (IT) security policy at the Panama Canal Industrial Control Systems (ICS)

Written by: Raúl Millán, Supervisor Specialist in Information Technology (Security), Unit of Security of Systems – TIGU, Executive VP of Technology and Information Technology, Panama Canal

Summary:

The process of developing and implementing a general IT security policy, intended to be followed by a non-IT related business unit, is always a challenge, because of this disconnect that typically exists between IT and the business. In the case of the Panama Canal, the "business" is defined as anything that has a direct relationship with a ship transiting the Canal's waters. This sets IT even further away from the "business", classifying it as a support unit, even though the Canal's operations are dependent on IT systems continuously, in the form of ICS (Industrial Control Systems).

Background:

In 2014, the importance of the revenue generating business units and the risks associated with the use of ICS was recognized by the Panama Canal. As a result, it was agreed that an IT security policy was needed to provide context and guidelines to the maritime, water, and energy business units in particular, all heavy users of ICS in their day-to-day operations.

These three units have different business goals, all aligned with income generation. The maritime operations unit is in charge of everything related to ship transits. The energy unit is tasked with generating the electricity required to run the Canal's maritime operations, as well as managing its output, which includes selling any excess capacity to the national energy market. The water business unit, has the responsibility of managing the water supply, which includes water needed for ship transit, as well as water used for human consumption. This is done either by selling fresh water from the lakes to the national water institute (IDAAN), or by processing the water through one of the water processing facilities owned and operated by the Canal.

While these three units currently represent the main revenue generating activities of the Canal, more are planned for the future to guarantee a profitable management of the Canal. Running the day-to-day operations without a clear guideline for securing their IT systems is simply not an option.

Analysis:

The requirement to develop an IT security policy to be applied to the revenue generating business units that design, deploy and operate Industrial Control Systems within the Panama Canal, was a finding contained in an internal audit; although the necessity of policy of this type had been identified a long time before the requirement was formalized by the auditors.

The main problem that the policy tried to address is the lack of clarity when it comes to the different roles and responsibilities related to the operation of the ICS environment. From the IT perspective there was no clarity regarding technical requirements (no participation in the purchasing process), no strategic training (little participation in knowledge transfer), lack of control of the design (designs usually don't consider basic IT security controls), and unfair support expectations from the business unit (IT is viewed as responsible and accountable for support). From the business perspective IT was viewed only as a support provider, even though, IT didn't always know what the business unit had chosen to implement.

Given this scenario, a gray area of unknown roles and responsibilities has been created, in which, neither of the two areas - IT and Operations - feel responsible for the maintenance, operations and security of the ISC. The main objective of the ICS security policy is to bring both IT and operations to the same level of understanding, when it comes to roles and responsibilities, IT security controls, and design models for ICS, for example the Purdue Enterprise Reference Architecture (PERA)[39]. It follows a standard structure for documents of this nature, and covers:

1. Definitions
2. Policy
3. Exceptions
4. Roles and responsibilities
5. Implementation

The definitions section includes numerous ICS-related terms, such as Operations Technology (OT), Supervisory control and data acquisition (SCADA), Distributed Control Systems (DCS), Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), Human Machine Interface (HMI), and the above mentioned PERA reference model.

The content part of the policy defines what is permitted and prohibited regarding:

1. Physical access to the areas where ICS is used, declaring mainly that means to restrict access to such facilities should exist.
2. Logical access to the ICS resources, describing typical IT control requirements (physical network segmentation, firewalls, IPS, authentication, logging, and whitelisting of devices).
3. Documentation and training are also included as responsibilities need to be assigned. Specifically the policy states that the documentation regarding the ICS should be considered confidential and should be protected according to the current policy for this type of information. In addition, cybersecurity training is mandatory to all operations and support personnel related to ICS.

39. www.en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

The policy also addressed the following areas more specifically:

A. Prohibitions:
1. Remote access
2. USB, external hard drives, cameras and smartphones
3. Wireless networks and cellular hotspots

B. Responsibilities assigned to the operational unit (system owner):
1. Inventory: keeping track of all authorized IT assets.
2. Documentation
3. Business continuity planning
4. Configuration change control

C. Responsibilities assigned to the IT security unit:
1. IT security incidents and vulnerability management
2. Security control operations (firewalls, IPS, endpoint security, network access control, and others)
3. Cybersecurity training
4. Network interconnection design

More specifically, as it relates to IT support activities, it was agreed that these should be executed by specifically assigned IT personnel through formal operational level agreements[40] with the business units. This approach clearly set the expectation for what the 'business' was to implement, as well as for the 'service' they were to receive from IT.

It is clear from the description of the policy that it sticks to the basics and does not go into details of how to implement the different controls, although it does describe the responsibilities of each player. This might be a departure from the typical IT policy, but since its aim was to address the gray area created by the lack of understanding of the different roles and responsibilities, it seemed like the best way to initiate the dialogue between IT and operations, regarding the security of ICS.

40. www.en.wikipedia.org/wiki/Operational-level_agreement

Lessons learned:

The most important lesson identified was the realization that the order in which the policy was developed was counterproductive. It quickly became clear that the roles and responsibilities should have been defined and understood before the policy was written. Although we purposefully made this decision, this approach is not recommended for the development of any IT policy. Its main risk lies in the fact that if the policy becomes outdated before the defined roles are established, the different business units might not be as willing to absorb the responsibilities perceived as "new obligations".

Instead, an IT steering committee should be put in place first. The committee can define the roles and responsibilities needed, as well as be a venue to discuss technical controls. Its particular value lies in ensuring that the specifics of OT security are discussed and agreed with the business units who own the ICS. It should be a permanent entity and it should not be confused with the IT security steering committees usually found within organizations. This is because the primary goal of OT will always be availability, while the general IT security goals tend to be guided by confidentiality and integrity. Therefore, it is recommended that an agreement should be reached before the development of a policy of any kind.
Ensuring the definitions are clear before writing the policy is critical, as is starting on this path early. Early adoption will help avoid a rush towards compliance with internal or external audits and regulations, depending on the industry. The main IT security goal should be achieving assurance, and not solely compliance. If the development of the policy is rushed, the result could be a document focused on compliance, rather than securing the systems against attacks.

An inevitable lesson learned was that sufficient time should be allotted for frequent face-to-face meetings to ensure buy-in and be able to explain the motives that drove the development of the policy. Rationale, as well as roles and responsibilities, should be documented and clear to everyone involved in the design, operation, and support of these systems.

Another important lesson was that cooperation from peers in the IT security community that face similar challenges can be particularly helpful. In the case of the Panama Canal, the resources that were available as a result of the development of the National Cybersecurity Strategy, which defined the various critical infrastructure actors, have been utilized. Moreover, today, the Panama Canal is cooperating with the Instituto de Acueductos y Alcantarillados Nacionales (IDAAN) to support them in developing their own ICS IT security policy, and to get feedback on our own approach. In conclusion, the lessons derived from the implementation of our IT security policy can be summarized as follows:

1. Establish a steering committee before developing the policy;
2. Define the objectives of the policy at the onset;
3. Engage in face-to-face meetings with business units on a regular basis;
4. A National Cybersecurity Strategy can help facilitate the process; and
5. Cooperation with peers is a critical step for success.

Cybersecurity is vital to protecting critical infrastructure

Author: Kaja Ciglic,
Director, Government Cybersecurity Policy and Strategy,
Microsoft

Extract

The essential nature of critical infrastructure sectors renders their protection an important concern for national policy. However, protecting connected critical infrastructure environments requires a new approach, substantially different from established practices used for traditional, offline security risks.

Technology is increasingly central to the social and economic opportunities of the world today. This is also true of national critical infrastructure. These entities are embracing digital connectivity and leveraging it to drive down costs, increase productivity and efficiency, improve service delivery, and ultimately enable greater economic opportunity. From financial services to emergency response, from energy generation to water supply, critical infrastructure sectors are using technology to fundamentally impact and continuously improve our quality of life.

The essential nature of the functions and services of critical infrastructure sectors renders their protection an important national policy priority. However, protecting connected critical infrastructure environments requires a different approach than that used for traditional, offline security risks, which could often be mitigated through regulatory action alone. The complexities of understanding and managing risk in connected environments can only be navigated through unprecedented coordination and collaboration between government, critical infrastructure owners and operators, and technology vendors.

Cybersecurity needs to incorporate risk management?

Microsoft's focus on cybersecurity spans over four decades. We make strategic decisions to advance the security of our products and services, including a $1 billion annual investment in research and development in this space. We also draw on our experience to regularly provide guidance and training to customers to protect themselves, and partner with governments globally to share best practices that help them fulfil their unique obligations to their citizens in cyberspace.

The guidance that Microsoft provides most frequently, irrespective of whether to public or private sector organizations, is that any cybersecurity approach must be based on prioritized risk management. All organizations, including designated critical infrastructure, must balance investments in cybersecurity with those that support other organizational functions, such as business development and new or improved products or services. No organization has an unlimited security budget, and all activities involve some degree of risk.

Policy frameworks that nations adopt with the aim of increasing critical infrastructure protection must therefore be based in prioritized risk management. They should enable organizations to identify and assess their most important cybersecurity risks, focusing on vulnerabilities, internal and external threats, and possible consequences of vulnerabilities being exploited. Moreover, they should enable organizations to determine how to manage the risk they have identified, including by accepting, mitigating, transferring or avoiding it.

What are effective security baselines?

Effective and efficient security baselines tend to adopt the following approaches:

- Bring together and utilize diverse expertise through an open, collaborative, and iterative development process
- Leverage existing best practices
- Help manage cybersecurity by underscoring prioritized risk management
- Facilitate decision-making by increasing understanding of cybersecurity management both within and between organizations
- Enable innovation by focusing on desired security outcomes rather than prescriptive requirements.

Governments can do so most effectively by utilizing policy frameworks that set security baselines for critical sectors. These can take form of voluntary guidance, coupled with incentives (e.g. procurement requirements or tax subsidies); or be implemented through a mandatory regulatory requirement, particularly when an elevated need for assurance arises from the risk environment. Irrespective of approach, the use of cross-sector security baselines will drive positive behavior beyond those organizations directly impacted, compelling or incentivizing suppliers to implement the same baseline activities as well[41].

Security Baselines best practice: NIST Cybersecurity Framework

The Framework for Improving Critical Infrastructure Cybersecurity, developed by the United States National Institute of Standards and Technology (NIST), is an example of a security baseline that has proven to be effective and has therefore quickly gained wider adoption, both in and outside the United States. Its usefulness can, at least in part, be attributed to the nature of its development process. The Framework was developed in close collaboration with industry – across different sectors and sizes – in an open, iterative, and consultative process.

The NIST Cybersecurity Framework was initiated by Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, issued on February 12, 2013. Its development took place over many months through official consultations, workshops, and informal conversations that took place all over the United States. The Framework continues to evolve and be updated, as through implementation stakeholders discover challenges or areas to which it could expand to help them manage their cybersecurity risk environment.

Critically, the United States is not the only geography looking to utilize the Framework. In Europe, the Italian government in 2015 adopted their own cybersecurity framework, which focuses on small and medium sized enterprises. The Italian document is largely grounded in the NIST Cybersecurity Framework. Similarly, the Australian Securities and Investments Commission (ASIC) in 2015 issued its Cyber resilience report: Health check (REP 429), which encouraged businesses to consider using the NIST Cybersecurity Framework to assess and mitigate their cyber risks.

The uptake of the Framework is likely to continue. The recent Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure mandates the use of the Framework across the agencies of the United States government. Moreover, the International Standards Organization (ISO) has recently approved work on a technical report on "Cybersecurity and ISO and IEC Standards", which seeks to adapt the Framework to the international environment, in part by incorporating many more ISO/IEC standards into its structure and informative references. We encourage governments across Americas to participate in that process.

41. -NIST Framework for Improving Critical Infrastructure Cybersecurity: www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
-Executive Order 13636 on Improving Critical Infrastructure Cybersecurity: www.obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
-Italian Cybersecurity Framework: www.cybersecurityframework.it/en
-ASIC Report 429 Cyber resilience: Health check: www.download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf
-Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

Security baselines as a central component of effective critical infrastructure protection

Security baselines are a foundational set of policies, outcomes, activities, practices, standards, and controls intended to help manage cybersecurity risk. They generally cover a wide range of risk management policy goals, such as protecting against cyber threats or detecting and responding to incidents. They can also include more specific desired outcomes (e.g., know your organizational risks), security activities or practices (e.g., conduct a risk assessment; document, review, and disseminate the results; and update the assessment regularly), and security controls (e.g., security policies are defined, approved by management, published, and communicated to employees and third parties).

Security baselines are particularly useful in improving cybersecurity because they can cover a range of risks that are typically applicable across a variety of environments, including different critical sectors. Most risks faced by governments and enterprises are similar, so most "baseline" or fundamental risk management and mitigation activities are also similar. For example, all organizations need to think about regularly reviewing and updating risk assessments, managing how resources are accessed to prevent unauthorized users or behaviors, and planning for and mitigating the impact of incidents. While security baselines should be applicable across sectors, enabling common understanding and consistent practice across interdependent organizations, they may also be complemented by sector-specific practices or standards that are responsive to sector-specific threats or vulnerabilities.

When security baselines are outcome-focused, they allow organizations to adapt to changes in technology and the threat landscape. Whereas prescriptive approaches mandate the use of particular technologies or controls (e.g., use two-factor authentication), outcome-focused approaches enable organizations to determine which technologies, controls, or other activities will enable them to meet, or even exceed, a set of desired security outcomes (e.g., control logical access to resources). As technologies and architectures evolve, those organizations can then implement new services and capabilities, including improved security services or capabilities responsive to new threats, with greater agility.

Leveraging international best practices safeguards limited resources

An important difference in handling the security of physical infrastructures and managing cybersecurity of critical infrastructures connected to the Internet is the inability of governments to limit their efforts to the confines of their national borders. It is imprudent to think of cybersecurity threats as solely national threats. From the banking sector to the energy grid, critical infrastructure sectors today are interconnected and operating internationally. Leveraging established international cybersecurity best practices, such as security baselines, can therefore ensure that interconnected or even interdependent global organizations and activities are supported or even strengthened by consistent approaches to cybersecurity risk management.

The process of building out a set of risk management practices from scratch is also resource intensive. In the light of the global shortage of cybersecurity professionals, this can be especially challenging. Utilizing tried and true methods therefore provides governments with a solid base of practices and more immediate results. It also ensures that sufficient resources are actually applied to security and risk management rather than diverted to compliance.

Achieving cyber resilience requires continuous commitment

Critical information protection is sometimes viewed narrowly, by solely focusing on developing policies and basic technical capabilities required for protection from, detection of and response to cyber-attacks. However, while an effective implementation of these will increase the security of infrastructure at a particular point in time, it is not sufficient. Critical infrastructure protection cannot and should not be viewed as an end state, but as a continuous process of managing risks to improve cybersecurity and resilience.

Cyber resilience can best be understood as an organization's capacities and capabilities for readiness, response, and reinvention in the face of a cyber threat. Effectively, this includes processes that enable stability, ensure recovery and help restore services rapidly. It is distinct from cybersecurity, as the latter focuses particularly on protecting the confidentiality, integrity, and availability of data, ICT systems, and ICT infrastructure, as highlighted above. Cyber resilience, on the other hand, is about an ICT system's ability to continue delivering as intended, even if cybersecurity is failing or has failed.

As a result, achieving cyber resilience requires comprehensive preparedness for events that are not just online, but can also include a physical attack, natural disaster, technical breakdown, human error, or any combination therein. It also requires a shift in thinking from traditional critical infrastructure protection to successfully managing risks and incidents through operational response, designed for continuous learning and reinvention.

The focus on the continuity of risk management is critical in this regard. Looking at critical infrastructure protection through this lens allows organizations to better plan for and manage the cybersecurity lifecycle, respond to threats as they evolve, internalize lessons learnt, and share them with the different operational and business stakeholders within the affected organization, as well as with policy and security communities outside the actual organization that could benefit from it.

Key components of cyber resilience

- Readiness.
  To plan for long-term readiness, an organization must identify assets, assess and manage infrastructure risk, develop capabilities to respond to and recover from disruptions, and invest in research, education, and practices that contribute to long-term cyber-resilience goals.

- Response.
  Using the plans and strategies set in place during the readiness phase, resilient entities continue to function during a crisis and rebound quickly. A resilient response is also adaptive and flexible: innovating during a crisis is a key element of resilience.

- Reinvention.
  Learning from and improving on existing plans and strategies is a hallmark of cyber resilience. After a crisis has passed, analysis is key: identifying what was effective and where the response was problematic; developing a plan for improvement; and then implementing that plan. It's important to think beyond short-term gains.

Public private partnerships allow for rapid response

Effective critical infrastructure protection needs to be grounded in private-private and also public-private partnerships. Governments, critical infrastructure owners and operators, and ICT vendors need to partner across sectors and across borders to be able to better manage risk. The benefits of collective action in cybersecurity are apparent. Information sharing is one example of the potential value of collective response to cyber threats. When information about attackers and methods of attack is shared, organizations are better prepared to thwart them. Governments would therefore be well served to consider implementing frameworks and incentives that would encourage critical infrastructure organizations to engage in this activity.

However, public-private partnerships can be effective beyond the basic sharing of actionable threat information. Through working groups or advisory committees, governments can bring different stakeholders together to improve the security of their critical services. Their focus areas could include: coming to an agreement on common cybersecurity baselines, establishing effective coordinating structures and information-sharing processes and protocols, identifying and exchanging ideas, approaches, and best practices for improving security, as well as improving international coordination.

These efforts do not always have to take place in formal structures. To leverage and integrate diverse expertise, governments should also focus on being open and collaborative, thereby creating an opportunity for an exchange of experiences, perspectives, and ideas. For example, when it comes to policy development, we found that cybersecurity policies benefit from an iterative process, which seeks to refine requirements over time and provides ample opportunity for feedback on draft plans.

Globally, dozens of countries are developing or evolving cybersecurity guidelines, regulations, and standards that seek to improve cybersecurity of their critical infrastructure. Security baselines, information sharing frameworks, and public-private partnerships are central to most of them. We hope that this publication will help guide cybersecurity policy development across the Americas in a way that results not only in the improved security and resilience of critical infrastructure, but also in continued societal opportunity and economic growth. Microsoft stands ready to support those efforts.

Industrial Cybersecurity and the Challenge of Cooperation between IT and OT in the Oil and Gas Industry

Author: Hernán Vázquez,
IT Manager of ARPEL

Extract

Today we face numerous technical challenges posed by the increasing importance of the digital world for the oil and gas industry. Moreover, digital transformation has resulted in organizational changes, as well as differing responsibilities related to regulatory compliance. This submission investigates some of these challenges and puts forward proposals on how to overcome them.

The comprehensive, real time use of information generated by business teams and field and/or plant teams, for example in digital oil fields, is becoming increasingly important for companies in the oil and gas industry. As elsewhere, the need has arisen for the Regional Association of Oil, Gas and Biofuels Sector Companies in Latin America and the Caribbean (ARPEL) and its members to integrate the information technology (IT) and operational technology (OT) worlds. Moreover, we identified a clear need for a space to build mutual understanding, exchange experiences and best practices, and address the challenges of cybersecurity together.

ARPEL membership currently represents over 90% of the upstream and downstream activities in Latin America and the Caribbean, and includes national and international operating companies, providers of technology, goods and services for the value chain, and national and international institutions in the sector. Our members face different realities, which became evident during the meetings organized by the Association in the past two years, however we have been also been able to observe the existence of common problems, such as those relating to the convergence between the IT and OT areas.

The OT world often includes specialized machinery, such as industrial control systems. Examples include drilling and refining equipment for the oil and gas industry, large networks of electrical systems, and sensors used in the energy sector and public utilities. These typically physical systems now integrate smart sensors that can help operations personnel increase their efficiency, save money, and make better business decisions. Indeed, when the data from the remote sensors is made available to a particular company, it becomes a powerful tool to ensure decisions are more effective, and ensure competitive differentiation. Therefore, instead of considering OT and IT as two individual networks, professionals in charge of these areas (chief information officers (CIOs), chief technology officers (CTOs) and chief information security officers (CISOs)) are realizing these two areas need to converge, which in turn introduces new challenges and opportunities.

The Industrial Cybersecurity Working Group of our Association decided to address this important challenge by organizing events, workshops, seminars, and webinars. These led us to conclude that further joint work is needed, involving both the OT and IT professionals, for example by conducting analyses and developing infrastructure security strategies. Moreover, we believe it is key for all countries in the region to adopt a formal regulatory framework for this field to ensure they are able manage this risk appropriately. In addition, the importance of incorporating cybersecurity into the agendas of company senior management was also noted.

As an example of such activity, one of our member companies set up an interdisciplinary cybersecurity committee made up of the main contact points for the various vertical businesses, and personnel of information systems and information security units. This committee published the first industrial cybersecurity standard in the company, thus starting it on the path towards integration of the IT and OT areas. In the process they leveraged the collaborative synergies of these areas, and developed special rules for each business group. The autonomous and active participation of the information security unit in security governance is vital to the integration of the various business areas within information systems management.

In addition to other important factors, the integration of IT and OT drives and justifies the need for information security management that is autonomous and separate from the information systems unit. Indeed, given the growing importance of the subject, it is essential that companies earmark more funds for cybersecurity, understanding that this is a long-term investment in risk mitigation for the company. This is increasingly true for large corporations.

The World Economic Forum[42] lists cyber risks as one of the most significant risks globally. Similarly, the Allianz Group places cyber risk in the top 10 of current major risks. Importantly, cyber risk has been growing in importance according to this index: jumping from position 13 in 2013 to 3 in 2017[43]. These data points are further proof that it is extremely important for corporate senior management to support the training of cybersecurity personnel, become involved in the development of company awareness programs, encourage the establishment of emergency response teams, and ensure periodic monitoring of infrastructure and systems.

Many of the issues outlined above were addressed in a study carried out in Argentina by the Industrial Cybersecurity Center of Spain[44]. It investigated 18 companies from different sectors and was released in 2016 at a seminar organized by ARPEL, the OAS and the Ministries of Foreign Affairs and Worship of the Republic of Argentina. The main findings included:

- For 42% of respondents, the IT unit was responsible for cybersecurity;
- The level training was acceptable in IT, although it was low in other areas, such as inhuman resources, quality control, procurement, and security.
- 41% of respondents did conducted a formal cybersecurity risk analysis;
- New projects generally included cybersecurity requirements, but these tended to be basic, or were delegated to the supplier.
- More than 50% of respondents had no incident management process in place;
- The study also uncovered that the private sector is largely unaware of public sector initiatives.

In addition to the findings highlighted above, it is appropriate to assume that there are further gaps in terms of awareness and knowledge of threats, training, risk analysis and incident management. However, even with that in mind, standards, understanding, best practices, and tools are already available that can help lower the likelihood of a cyberattack. Cyberattacks are a manageable threat, and the key to being prepared lies in being able to implement such standards and good practices correctly.

In ARPEL, we will continue to partner with our member companies, member institutions, and national and international agencies with the aim of reducing the existing gaps and achieving operational and management excellence on an issue as important as cybersecurity.

42. World Economic Forum, Global Risk Report (2018): www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready/

43. Allianz Risk Barometer; Top Business Risks (2017): www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

44. Industrial Cybersecurity Center of Spain: www.cci-es.org/web/cci/home

Creating a global awareness of Critical Information Infrastructure Protection- the Meridian Annual Conference: over a decade of experience.

Author: Peter Burnett,
Meridian Process

Extract

This submission provides a brief discussion of the importance of CIIP and Meridian's role in promoting that awareness around the world. It draws parallels with the London process and distinguishes CIIP from cybersecurity.

Background

In 2005, very few people had heard of cybersecurity. Many people thought that their critical infrastructure (if they even recognized that concept) could be protected by fences, guards, access control systems etc. In fact, some of the most important elements of our critical infrastructures were already heavily dependent on ICT at the time, especially in the finance, energy, and of course, telecommunications sectors. We used to talk about electronic attacks, computer security, information security, but when these concepts were applied to the protection of critical infrastructure, they became known as Critical Information Infrastructure (CII) Protection – the protection of the information aspects of the critical infrastructure.

Five years later it became evident to many countries that there was a whole raft of important security issues relating to the use of ICT across many aspects of our lives, and the term which emerged to cover these was cybersecurity. This was when the UK's Foreign Secretary established the series of high-level conferences known initially as 'The London Process', but now better known as the Global Conference on Cyber Space (GCCS). That series of Ministerial level events stimulated governments of many countries to find out more about, and acknowledge the importance of, cybersecurity. It became accepted practice that countries should create national cyber security strategies (NCSS) to tackle the cybersecurity aspects of economic development, defense and privacy, to name but a few issues.

Awareness Raising

There can be little doubt that the GCCS has done a great service in transforming cybersecurity from a technical subject to a political one, boosting its importance on government agendas. Hosted by India in November 2017, the GCCS 2017[45] aimed to promote an inclusive cyberspace with a focus on policies and frameworks for inclusivity, sustainability, development, security, safety and freedom, technology and partnerships for upholding digital democracy, and advocating dialogue among stakeholders.

This high-level activity has also encouraged many governments and organizations to address the inequality between countries in terms of their cybersecurity maturity, and to engage in cybersecurity capacity building. The OAS is a prime example of such an organization, and they have made a huge contribution to raising cybersecurity awareness and capacity of many countries across the Americas and the Caribbean. The OAS has also been a highly valued supporter of Meridian, particularly when Meridian's annual conference has taken place in the OAS region. There may be several reasons why the OAS supports Meridian, but one reason is the role that Meridian has developed in terms of cybersecurity capacity building.

Long before the first Meridian conference was organized by the UK's CIIP agency, the National Infrastructure Security Coordination Centre (NISCC) in Greenwich, London in 2005, a few key ideas had been developed within NISCC:

1. Governments realized that they knew very little about how to actually protect their CII. Consequently, the concept of trusted information sharing evolved, where government and industry operators of CII would share their information, experiences and ideas, confidentially, to help protect against threats, for mutual benefit. This is now a well-established concept and practice, but it is still just as important, and just as difficult, to do successfully.

2. The second realization was that, unlike the protection of critical Infrastructure which had been a largely national activity, CIIP needs to be addressed on an international basis. This is because CIIs are almost always interconnected across borders, and therefore it is in the interest of every country to help protect the CIIs of other countries. A vulnerable CII in one country can create an attack path to other CIIs – like a weak link in a chain. Moreover, the advent of cyberspace means that every country now has a digital border with every other country in cyberspace.

There are of course many reasons to confer with other countries about CIIP, for example: to share information about developments and best practices in response, exercises, policies, strategies, research, legislation etc. and, of course, developments in technology. Meridian has provided a forum for this at its annual conference for 13 years, and these events are specifically engineered to encourage an exchange and discussion of ideas, practices, and views in an informal non-political and confidential environment. It also provides opportunities for delegates to establish and develop trusted links with their counterparts in other countries. These personal connections can prove invaluable when dealing with contingencies and emerging threats, especially when they are developed at the policy working level, which exemplifies Meridian delegates and Meridian community members.

This is one area where Meridian differs from GCCS, although there are a number of parallels between the two series of conferences and the accompanying processes. Meridian delegates are typically senior government policy officials, not the ministerial level delegates who are the target delegates at GCCS,

45. Experiences and Good Practices-Case Studies

though Meridian members often attend GCCS in support. Meridian conferences are much smaller and more intimate events, with usually no more than 100 delegates in total, and no more than 3 per country, not the vast delegations who populate GCCS. This helps all Meridian delegates to mix together and develop trusted links.

The other big difference is that Meridian focuses on CIIP and does not attempt to address the much broader field of cybersecurity. This allows a much clearer focus, without the distraction or diversion into the myriad elements of cybersecurity. It had originally been assumed that CIIP would simply be subsumed into cybersecurity, when that became a fashionable subject on government agendas. In practice, however, there is still a very strong discrete interest in CIIP amongst developed nations, where it is often arguably considered the most important element of cybersecurity. This is because if a nation's CII is not protected, then all other aspects of the online environment are at risk, and so is the very security and safety of that nation.

The continuing existence of a globally respected forum dedicated to CIIP underscores the importance of the subject. The fact that Meridian continues to flourish in its 13th year is all the more remarkable since it remains a government-only forum, in order to preserve its confidential atmosphere. That means that Meridian has no industry sponsorship or support and therefore minimal resources, and no secretariat except for a part-time coordinator. Nonetheless, there has always been a long list of countries wishing to host the annual conference, and since 2015 there has been support from GFCE in the form of the GFCE-Meridian CIIP Initiative, as well as key contributions from specific governments, including Sweden, UK and Netherlands.

Meridian has deliberately followed a policy of rotating the hosting of Meridian in different regions, whenever possible. This means that it has now been hosted 3 times in the Americas. In 2009, it was hosted by USA, in 2013 by Argentina, and 2016 by Mexico, and it is likely to be back in the Americas again before long.

One of the big benefits of hosting Meridian is that it raises the profile of CIIP on the governmental agenda of the host country. This is because the host agency will invite delegates from other agencies, stimulating a debate about which agencies have a role in CIIP, and how they can all work together. This was a unique observation when Meridian was hosted in Buenos Aires, but it has also been true for many other host countries. Hosting Meridian helps to build links within that region, and can boost the host country's efforts to show leadership in the subject. The crucial need for international liaison in CIIP makes the hosting of Meridian an extremely valuable way to establish working level contacts on CIIP issues with neighboring countries, as well as others among the 60 plus countries in the Meridian community.

Meridian now has other specific capacity building activities as well, supporting the continuing development of CIIP in all countries. These include the long-standing Meridian CIIP Directory of contacts, the more recent CIIP Good Practice Guide, as well as a new "Buddying Program" under development, and a CIIP training package currently in development. The best way to find out more about these developments, and to become a member of the Meridian Community (if your country has not already joined) is by accessing **www.meridianprocess.org.**

APPENDIX
Additional Resources

Several entities, such as the Global Forum on Cyber Expertise, the U.S. American National Institute of Standards and Technology, as well as companies like Microsoft, have developed guidelines to support development and implementation of CIIP strategies and approaches, as well as associated frameworks for assessing and managing risk in relation to CII. These can be applied in both the public and private sectors:

- GFCE (2016): The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers[46];
- National Institute of Standards and Technology (NIST) (2017): Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1 Draft 2)[47];
- Microsoft (n.d.): A Framework for Critical Information Infrastructure Risk Management[48];

While the first guide covers the development of a CIIP strategy from a policy perspective, the next two offer specific recommendations relating to the implementation of CIIP initiatives. In particular they provide guidance on how to assess and manage cybersecurity risks. The final document provides specific recommendations as to how to develop and implement basic security requirements to ensure organizations can remain secure. In addition, sector specific organizations that count as critical infrastructures, both public and private, have developed risk management guidance for their vertical industries. These include, for example, the North American Electric Reliability Corporation Critical Infrastructure Protection Committee[49], Chemical Industry Data Exchange/American Chemistry Council[50], and the Financial Stability Board[51].

Finally, the International Standardisation Organisation (ISO) provides several guidelines, including: ISO 27032, which provides guidance for improving cybersecurity and covers baseline security practices; ISO 27001, which supports the establishment of an Information Security Management System (ISMS) in an organization; and ISO 27005, which highlights best practices for development of a risk management methodology.[52]

46. GFCE-MERIDIAN, Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers: www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

47. NIST, Framework for Improving Critical Infrastructure Cybersecurity: www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

48. Microsoft, A Framework for Critical Information Infrastructure Risk Management: www.uery.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc7

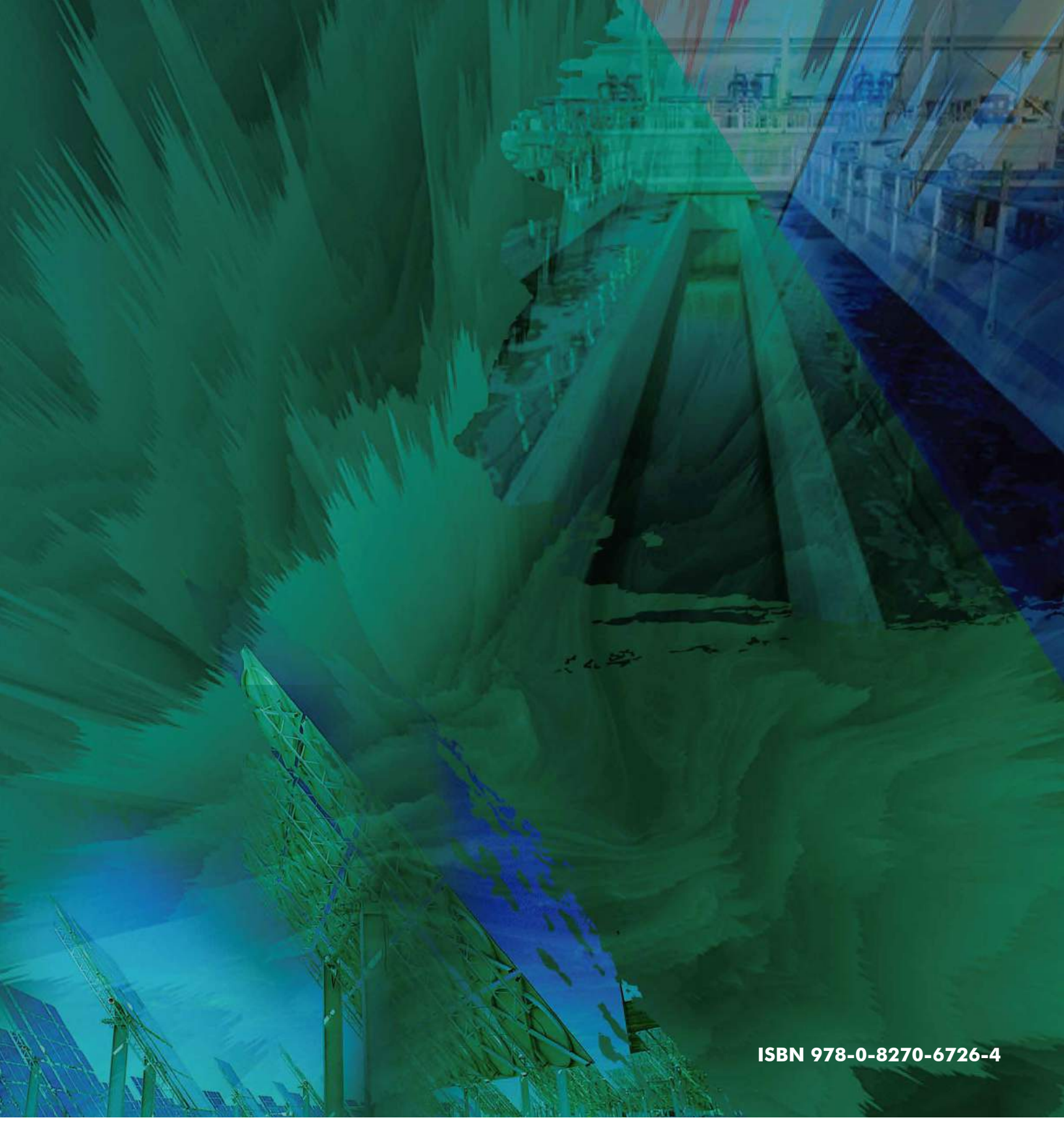
49. North American Electric Reliability Corporation Critical Infrastructure: www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

50. Chemical Industry Data Exchange/American Chemistry Council: www.chemitc.americanchemistry.com/RCSC-NIST-Framework-Guidance-Jan-2016.pdf

51. Financial Stability Board: www.fsb.org/wp-content/uploads/P131017-2.pdf

52. ISO. (2011). ISO/IEC 27005:2011: Information security risk management: www.iso.org/standard/56742.html; ISO. (2012). ISO/IEC 27032:2012:Guidelines for cybersecurity: www.iso.org/standard/44375.html; ISO. (2013). ISO/IEC 27000: Information security management systems: www.iso.org/isoiec-27001-information-security.html

CRITICAL INFRASTRUCTURE PROTECTION IN LATIN AMERICA AND THE CARIBBEAN 2018



ISBN 978-0-8270-6726-4

OAS More rights for more people

Microsoft