TREND MICRO™

Organization of American States

Report on Cybersecurity and Critical Infrastructure in the Americas

Contents

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

ORGANIZATION OF AMERICAN STATES LEGAL DISCLAIMER

The information and arguments expressed in this report do not necessarily reflect the official views of the Organization of American States or the governments of its Member States.

Message from OAS Assistant Secretary General

Ambassador Albert R. Ramdin

The Organization of American States (OAS) works with our Member States to strengthen their cybersecurity capabilities, particularly to protect critical infrastructure. In 2004, the General Assembly of the OAS unanimously passed the Comprehensive Inter-American Cybersecurity Strategy. Recognizing that since then cyber threats have persistently grown, the government of the Americas signed the declaration on “Strengthening Cyber Security in the Americas” (2012) and more recently, the Inter-American Committee against Terrorism (CICTE) of the OAS adopted the “Declaration on the Protection of Critical Infrastructure from Emerging Threats” (2015). These instruments are critical for the promotion of cybersecurity policies to improve cybersecurity in critical infrastructure in the Americas.

Member States rely on critical infrastructure to provide essential services and products, and as countries of the Americas have experienced a growth in the number of infrastructures running on Internet-facing networks, so the number of cyber-attacks to the same infrastructures has increased, which could compromise a country’s critical infrastructure and ability to provide essential services to its citizens.

Exploitations that can affect countries’ infrastructure are usually infiltrated by simple or sophisticated tools that can access mobile and other personal devices to infiltrate high-value sectors, such as transportation, energy, or financial systems. To tackle these cyber threats, the OAS began its efforts to strengthen cybersecurity capacities in critical infrastructure by providing tailored trainings to management-level officials, policymakers, and security technicians working at countries’ critical infrastructure.

Over the years, these efforts have evolved to also better depict the current attack trends in critical infrastructure. Understanding Member States' cybersecurity capacities and cyber attack trends is the first step in strengthening response capacity. Bearing this in mind, this report was prepared for the purpose of being a comprehensive document from which Member States, critical infrastructure operators and other can draw useful conclusions and gain a better understanding of major cyber threats affecting critical infrastructure in the Americas. For instance, the data gathered revealed that 53% of the respondents noticed an increase of attacks to their computer systems in 2014, and 76% stated that cyber attacks against infrastructure are getting more sophisticated.

It is noteworthy that the data gathered was only possible thanks to the cooperation that the OAS encourages between public and private sector. Governments must work together with the private sector and civil society organizations, recognizing that cybersecurity is a shared responsibility. This report is a great example of multi-stakeholder approach adopted by the OAS in its cybersecurity policies, combining contributions from Member State governments, the private sector, academia and civil society. We hope this information will guide our region in providing a more secure cyberspace and in improving cybersecurity capacities to protection our essential infrastructure.

Foreword

Organization of American States

Adam Blackwell

Secretary for Multidimensional Security | Organization of American States

The world has never been smaller, with more of us connected at even higher Internet speeds than ever before. The Internet of Things (IoT) has changed the way we interface with each other, revolutionized business processes, and altered the way in which countries and critical infrastructure are operated.

There is no doubt that this hyper-connectivity is a powerful development tool and opportunity for growth for governments, business, and individuals alike—a tool that must remain open and accessible despite the inherent risks. The challenge lies in our ability to balance and manage these risks for the foreseeable future. The openness and ease of access of a hyper-connectivity has lowered the barriers to entry for criminal entrepreneurs as they can participate in illicit activities from almost anywhere. This makes it difficult for law enforcement to link the crime to the perpetrator and jurisdiction.

Consequently, governments, international organizations, the private sector, and civil society must all work together in reinforcing collaboration and recognizing that cybersecurity is a shared responsibility. Cybercrime affects society as a whole; not only threatens individuals' privacy, but it may also potentially compromise a country's critical infrastructure and its ability to provide essential services to its citizens. The globalized nature of economies also means that it is a threat at an international level. This highlights the need for action on four different levels: international, national, private sector, and individual. Individuals, too, hold some responsibility and must be aware of their own vulnerabilities and involvement in cyber hygiene.

Latin America and the Caribbean currently have one of the fastest-growing Internet populations in the world, giving rise to a number of significant cybersecurity challenges. In response to the increasing threats, the OAS, through the Inter-American Committee Against Terrorism (CICTE), has developed a regional cybersecurity program focusing on strengthening cybersecurity and improving critical information infrastructure protection throughout the Americas. Recognizing the importance of collaboration, the OAS Cybersecurity Program revolves around the implementation of the following seven-point plan:

[1] Engaging civil society and the private sector: More than 80% of the infrastructure that drives the Internet and administers essential services is owned and operated by the private sector. For this reason the OAS has established partnerships with private sector companies such as Trend Micro, who we are pleased to be collaborating with on this report, Microsoft, Symantec as well as non-profit organizations including the World Economic Forum, STOP. THINK. CONNECT[1], and the Latin American and Caribbean Network Information Center.

[2] Raising awareness: With the development of IoT, people are connected to the Internet in many different ways. This new trend highlights the importance of designing policies to raise awareness among Internet end users about basic cybersecurity measures. The OAS has embarked on an aggressive awareness-raising program to make sure individuals understand the risks and the need to take appropriate measures for their own cybersecurity.

[1] http://stopthinkconnect.org/

[3] Developing national strategies: A national cybersecurity strategy allows countries to define a comprehensive vision on cybersecurity and set clear responsibilities, coordinating actions between governments, and relevant stakeholders. The OAS promotes the development of national cybersecurity strategies and frameworks in all Member States, working in the past with Colombia, Panama, and Trinidad and Tobago, and with others underway in Dominica and the Bahamas.

[4] Providing training: Remaining current is fundamental in the ever-evolving environment of cybersecurity. The delivery of technical training to officials has proven to be a highly successful means of enhancing cybersecurity at the national and regional levels. In particular, the OAS has assisted Member States in establishing robust national and governmental Computer Security Incident Response Teams (CSIRTs), whose numbers have risen from six to 19 in the last decade.

[5] Rehearsing crisis management: In parallel with technical training and the development of response teams, the OAS also conducts crisis management exercises. This allows Member States to tailor exercises to their own needs while strengthening collaboration at the technical level within other countries responding to threats.

[6] Carrying out technical assistance missions: The OAS responds to countries' needs by developing and carrying out technical assistance missions designed to address their concerns. This typically involves site visits, policy reviews and presentations by local authorities, culminating in a series of recommendations by experts.

[7] Sharing information: The OAS is working on the development of a network of national CSIRTs and other cybersecurity-related authorities, which aim to facilitate real-time communication and information sharing.

Trend Micro

At Trend Micro, our mission of making a world safe for exchanging digital information has naturally led us to develop and cultivate private/public partnerships with organizations around the globe. Never has it been more important for public and private organizations to collaborate and share information in an effort to combat cybercrime. To this aim, we are proud to have partnered with the OAS for the development of this report that examines cybercrime threats impacting the critical infrastructures of the Americas.

The data gathered in this report includes information from the Americas, all of which reported a significant increase in the level of incidents to their computer systems within the past year. The increase in criminal activity is of no surprise, as the trend of increasing cyber attacks in Latin America was documented in our 2013 report of Cybersecurity Trends and Government Responses in the region.[2]

[2] http://www.oas.org/cyber/documents/OASTrendMicroLAC_ENG.pdf

Moreover, the TrendLabs^{SM} 2014 Annual Security Roundup reports that numerous organizations worldwide, including banks and public utilities lost millions of customer records and credentials to attackers in 2014.[3] The critical infrastructure sector has emerged as an especially vulnerable attack vector, due to aging facilities and the prevalence of "bolt-on half-measures and Band-Aids," in lieu of comprehensive security systems.[4]

The report provides readers with a greater understanding of the kinds of attacks experienced by this sector in the Americas and brings attention to the need for increased collaboration between critical infrastructure organizations and governments. As we witnessed in 2014, the United States government has recognized the vulnerabilities in this sector and the possible grave consequences of not properly securing industries on a national scale, such as electrical grids, water and fuel supplies, and telecommunications.

This report is intended to shed light on cybercrime activity and trends that take place in the Americas within the critical infrastructure sector. It also aims to provide insight on how fostering collaboration between these industries and their governments can strengthen their ability to combat cyber attacks.

[3] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-magnified-losses-amplified-need-for-cyber-attack-preparedness.pdf

[4] http://blog.trendmicro.com/breaking-down-old-and-new-threats-to-critical-infrastructure/

Executive Summary

Attacks on critical infrastructure have become a growing cause of concern for governments and private providers around the globe—whether inflicted by cybercriminals seeking financial gain or by hackers as political acts aimed at undermining governments' and companies' credibility.

The trepidation around these threats is justified, as research demonstrates that attacks on critical infrastructure have increased in both prevalence and sophistication and will continue to grow in the near future.

Site management and monitoring has improved for critical infrastructure facilities as they have become more progressively connected to the Internet. The added convenience of connectivity, however, has turned the once-limited attack surface of these industries into a fertile landscape for cyber attacks. Due to the potentially high-profile effects of attacks to critical infrastructure systems, these industries have become even more attractive targets for cybercriminals.

Building on the success of our seminal joint 2013 study "Latin American and Caribbean Cybersecurity Trends and Government Responses", the OAS and Trend Micro have joined together to provide another view into the state of cybersecurity for OAS members.[5] This unprecedented survey of over 20 OAS Member States provides a view into the actual state of cybersecurity around critical infrastructure in the region and the threat trends these crucial organizations face.

The data collected provides important insights into the cyber attacks experienced by critical infrastructure organizations in the region, as well as organizations' cybersecurity measures and policies; collaboration with local governments; and their preparedness for cyber attacks. Many of the survey's findings correlate with our existing research on critical infrastructure attacks, and new insights will help to guide our research in the future as we work to protect this industry against cyber attacks.

The survey respondents came from government agencies, as well as critical industries such as communications, banking and finance, manufacturing, energy and security, among others. The respondents showed that attackers are as interested in data theft as causing chaos and mayhem by hacking control systems (SCADA).

Not surprisingly, spear-phishing tactics were cited by all responding members as the single biggest attack method they had to defend against, with the exploitation of unpatched vendor software vulnerabilities being a distant second. This mirrors the problematic role that spear phishing plays in cybersecurity incidents generally, most especially in targeted attacks.

[5] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Respondents made clear that attacks targeting infrastructure are a clear and present danger as only a clear minority of responding members could say they hadn’t seen these kinds of attacks.

In their response outlining the threat landscape, participants painted a picture that depicts the threat as being severe, while some perceived the future of securing these infrastructures as bleak. For the majority of respondents, attack frequency is increasing or holding steady, with attack sophistication dramatically evolving.

On the positive side, respondents indicated that they felt prepared or somewhat prepared to face a cyber attack. Organizations have put in place technologies, policies, and procedures that can help protect their environment.

The report highlights the lack of a proactive partnership between governments and private organizations in this region. A stark majority of respondents in both private industry and government reported either no dialogue or only informal dialogues between these key partners.

A seminal conclusion is that the lack of a public/private partnership represents a historic missed opportunity, albeit the level of trust for governments to advance a cybersecurity agenda around critical infrastructure is very high for all respondents.

The other clear threat to preparedness to meet these evolving threats is flat budgets. A clear majority of respondents reported challenges that can hamper their ongoing defense against attacks targeting critical infrastructures.

While organizations in the Americas have done good foundational work to protect critical infrastructure against attacks, a tipping point looms. As attacks continue or worsen in frequency and sophistication and focus not just on disrupting critical infrastructure but also compromising key information that could be used in the future, defenders may soon find themselves short in terms of the support necessary to stave off threats. The lack of funding and an unmet desire for government leadership in this area leaves defenders feeling increasingly left on their own. More than ever, governments in the region need to take the outstretched hands of those in critical infrastructure looking for help and lead them to help better protect against increasing attacks against this crucial sector.

Analysis and Commentary on the State of Cybersecurity in Critical Infrastructure in the Americas

This section provides a series of short essays by select expert contributors analyzing and commenting on the state of cybersecurity and critical infrastructure.

Information provided by Trend Micro

Trend Micro Forward-looking Threat Research has observed several trends over the past year. Among them, the most significant trend is the use of malware to compromise supervisory control and data acquisition (SCADA) systems, including Homeless Management Information System (HMIS), historians, and other connected devices.

This trend has manifested itself in two major ways: malware disguised as valid SCADA applications and malware used to scan and identify specific SCADA protocols. In the former, malware has been disguised as valid applications for Siemens, Allen Bradley, and several other vendors. In the latter manifestation, we have witnessed specific malware scanning for OPC and Modbus. While the reason for this scanning has not been determined, the purpose is likely intelligence gathering for industrial espionage or future targeting for an attack. We have observed increased interest in SCADA protocols, attacks and malware and expect this trend to continue.

This trend is unique in that there appears to be a noticeable growth of knowledge from attackers about SCADA technology. Not only have these attackers demonstrated knowledge of application names, project names, etc., they are also becoming very familiar with SCADA protocols. This knowledge has clearly grown month by month. This trend is expected to increase significantly in 2015 and 2016, with more functionality found in malware and additional groups attacking SCADA likely to be revealed.

Establishing the origin of these cybercriminal groups is often difficult, if not impossible. However, attribution provided by multiple intelligence firms (not including Trend Micro), has concluded that a majority of groups using targeted malware against SCADA systems has originated from Russia. The motivation is unknown; hence, it is difficult to determine whether these attacks are being conducted by individual cybercriminals or those backed by the government.

Two Noteworthy Critical Infrastructure Attacks of 2014

According to security firm CrowdStrike, a Russian hacker group called "Energetic Bear" caused significant disruption for companies in the United States in the energy sector.[6] The group used a highly-effective and newly-formed malware known as "Havex" to break into the industrial control system (ICS)/SCADA systems of their targeted companies. Once the Havex malware infects a company's ICS, it then relays sensitive company data and information back to the hackers through the command-and-control (C&C) servers. According to Mike Assante, Director of ICS at the SANS Institute, "ICS-capable malware modules (Havex and BlackEnergy II) indicate significant investments in time and money."

At the end of 2014, an attack launched against a steel plant in Germany resulted in physical damage, according to a report by the Germany's Federal Office for Information Security, or the BSI.[7] The attackers had apparently first compromised the steel mill's office network by using spear-phishing emails and clever social engineering. From there, they worked their way into the production network and other systems, including the systems that control the plant's equipment.

The compromise resulted in frequent failures of individual control components and the various systems, and ultimately led to the operators being unable to adequately regulate and promptly shut down a blast furnace. The result was "massive damage to the plant," the BSI noted.[8]

- Organizations can employ the following practices to help defend against ICS attacks in 2015:
- Deploying anti-malware software where possible throughout the ICS environment
- Using a bastion host to prevent unauthorized access to secure locations throughout the ICS environment
- Applying application whitelisting throughout the ICS environment to prevent unauthorized applications from running
- Deploying a breach detection system
- Enabling a USB lockdown on all SCADA environments. This prevents malware from physically entering the environment
- Deploying basic security measures in between network segments, such as firewalls/IPS, in between the business network, and the ICS network.

"A report by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in the United States reports that industrial control systems were hit by cyber attacks at least 245 times over a 12-month period, from October 2013 to September 2014. Around 32% of industries were from the energy sector, while critical manufacturing comprised 27%. ICS-CERT further revealed that 55% of investigated incidents showed signs that advanced persistent threats, or targeted attacks, had been used to breach systems."

References:

http://www.v3.co.uk/v3-uk/news/2399334/us-industrial-control-systems-attacked-245-times-in-12-months

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

[6] http://www.infosecurity-magazine.com/news/energetic-russian-bear-attacking-western-energy/

[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

[8] http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html

Caltech Smart Grid Research: Potential Cyber Threats and Mitigation

Steven Low

Professor of Computer Science and Electrical Engineering | California Institute of Technology

We are at the cusp of a historic transformation of our energy systems. The power network, from generation to transmission and distribution to consumption, will undergo the same kind of architectural transformation in the coming decades that computing and the communication network has gone through in the last two. We envision a future network with hundreds of millions of distributed energy resources (DERs) such as solar panels, wind turbines, electric vehicles, energy storage devices, smart buildings, smart appliances, smart inverters and other power electronics. These intelligent endpoints will not be merely passive loads, as are most endpoints today, but endpoints that may generate sense, compute, communicate, and actuate. They will create a tremendous opportunity for greater efficiency, flexibility and capacity in our generation and utilization of electricity. They will also create severe risks because of potential cyber attacks and other vulnerabilities.

Our research addresses some of the most fundamental and difficult engineering and economic challenges to help us understand and guide this historic transformation, as well as to mitigate its risk and realize its potential. In the following we provide a sample of our research results.

Attack and failure propagation and mitigation

The transformed power network will be the largest and most complex integration of cyber and physical networks in history. Intelligence will be embedded everywhere, from solar panels and electric vehicles to smart appliances and energy storage devices, from homes to micro-grids to substations. While indispensable for stability, reliability and efficiency of the network, this will also create new fragility to cyber-security threats. Each DER will become a potential entry point for a cyber attack. The cyber network that controls and optimizes the physical network will also greatly amplify the scale, speed, and complexity of an attack. It can also quicken and broaden failure propagation on the physical network, making blackout mitigation much more difficult.

We have studied this process to understand its dynamics and develop mitigation strategies. Suppose an attack against the cyber or physical network resulted in the failure of an initial set of grid devices. How will this failure propagate? Will the cascading failure lead to a large-scale blackout? Answering these questions requires an understanding of the redistribution of power flow on the grid when a set of grid devices fail.

We have discovered monotonicity properties with respect to link failure that allow us to systematically understand the dynamics of power redistribution as the cascading failure unfolds over the network. Utilizing these monotonicity properties, we have designed load shedding strategies that can mitigate network overload and blackouts as grid devices fail, and isolate potential cyberattacks.

"While indispensable for stability, reliability and efficiency of the network, this will also create new fragility to cyber-security threats. Each distributed energy resource will become a potential entry point for a cyber attack. The cyber network that controls and optimizes the physical network will also greatly amplify the scale, speed and complexity of an attack."

Power flow optimization

Optimal power flow (OPF) is the problem of minimizing certain cost functions, such as power loss over a network, the fuel cost of electricity generation, or security constraints. OPF is fundamental in power system operations and planning as it underlies numerous applications such as unit commitment (which generators to use), economic dispatch (how much these generators should generate), state estimation (estimation of the full network state from partial measurements), stability and reliability assessment (will the network converge to a new stable equilibrium in case of a contingency?), Volt-VAR control (provision of reactive power to stabilize voltages), and demand response (adaptation of load to fluctuating supply).

The optimal network is flexible, with assets that have time-varying dynamic ratings reflecting the asset capability under varying operating conditions. It is also optimally configured—opening or closing transmission lines becomes a decision variable, or control action, rather than an input to the problem, or state. When possible, the security constraints are corrective rather than preventive. With preventive security constraints, the system is operated conservatively to survive loss of any transmission element or generator. In contrast, corrective constraints reconfigure the system with fast-acting equipment such as special protection systems or remedial action schemes immediately following loss of a generator or transmission element, such as our load shedding strategies to mitigate potential cyber attacks.

In the last few years, we have been developing a novel approach to OPF through semidefinite relaxation. This method provides the ability to determine whether a solution is globally optimal. If it is not, the solution provides a lower bound on the minimum cost, and hence, a bound on the suboptimality gap of any feasible solution. We have tested our methods on various benchmark systems and real-world distribution systems, and found that they successfully provide optimal global solutions in more than 95% of the cases studied.

Ubiquitous load-side frequency control

Unlike data networks, supply and demand for electricity must be balanced at all times and at all points of the power network. This is achieved through frequency control. It maintains the frequency of our alternating current (AC) power system tightly around its nominal value (e.g., 60Hz in the US, 50Hz in Europe) when demand or supply fluctuates. The system dynamics are primarily driven by big rotating machines in bulk generators. The frequencies at which these machines rotate determine the frequency in the power network. When demand exceeds supply, these machines slow down and the system frequency drops. When demand falls short of supply, these machines speed up, and the system frequency rises.

Hence, the frequency deviation measures the instantaneous power imbalance.F

requency control is traditionally implemented on the generation side, i.e., generation is adjusted in response to demand fluctuations. We have been studying the possibility of ubiquitous continuous load-side frequency control. Unlike the traditional generation-side control, load-side frequency control responds faster and does not consume extra fuel or emit extra greenhouse gases.

Both the need and technologies for implementing load-side frequency control have matured in the last decade. The bottleneck problem is how to design real-time feedback control algorithms for ubiquitous continuous load-side frequency control.

We have recently developed a set of distributed algorithms that are provably stable, efficient, and fair, and can scale to millions of intelligent loads. Simulations have shown that they work in harmony with generator-side control, and improve both the steady-state and the transient behavior over generator-side-only control. As we transform our power network with integrated DERs, we can modify these algorithms to adjust for link failures that may be caused by cyber attacks.

Conclusion

Integration of cyber and physical networks holds the future promise of efficient, reliable and flexible supply of electrical power in harmony with rapidly evolving energy needs. Intelligent DERs will create tremendous opportunities, but also introduce potentially severe risks.

By understanding the engineering challenges and risks presented by these opportunities, it is possible to mitigate potential cybersecurity threats. Monotonicity properties of grid failures caused by possible cyber attacks can be utilized to develop load shedding strategies. Security constraints can be included in OPF formulas to maintain network efficiency. Additionally, ubiquitous load-side frequency control may be utilized to maintain network stability through distributed algorithms that adjust for potential cyberattacks.

The Vital Role of Critical Information Infrastructure Protection (CIIP) in Cybersecurity

Peter Burnett

Meridian Coordinator | CiviPol Consultant

Quarter House Ltd

Cybersecurity Information Sharing

CIIP is a subset of the more widely-known concept of Critical Infrastructure Protection (CIP), or the protection of the energy, telecommunications, water supply, transport, finance, health and other infrastructures that allow a nation to function. These critical infrastructures need to be protected against accidental and deliberate events that would stop them operating correctly and would severely impact the economic and social well-being of that nation.

These infrastructures have been protected against physical attack and sabotage for many decades up to the beginning of this century. However, a number of countries realized that many of these critical infrastructures also had a common component: they were dependent on a greater or lesser degree on information infrastructures, (telecommunications networks and computer systems, ICT).
It was because of this dependency that the discipline of Critical Information Infrastructure Protection (CIIP) was born. That realization has grown rapidly amongst governments and industries, and along the way, the broader concept of cybersecurity has now emerged which includes CIIP.

CIP (including CIIP) is essentially a problem for governments to manage, but the failure of CIP is a problem for everyone as we are all dependent on that infrastructure. CIP is often a national responsibility, and can be largely managed as a national security issue, but CIIP is almost always an international or global issue. There are few (if any) countries whose telecommunications infrastructure does not extend across their borders, and in cyberspace you have a border with every other country, not just your neighbors.

In many countries, especially western ones, critical infrastructures are privately owned and run by private critical infrastructure operators, and the information infrastructures are often run by multinational corporations based outside the borders. This means that governments must work closely with those private sector infrastructure operators to ensure continuity of service by building resilient infrastructures. The Internet was intentionally conceived to be a resilient network, and fundamentally it still is. It was never designed to be such a vital critical information infrastructure as it has now become, especially to small businesses, whose dependence on email, websites, cloud access other online resources increases every day. The impact of a serious loss of Internet access for a prolonged period is incalculable due to the complexity of our dependencies. Try just losing broadband for a few weeks!

It is therefore essential for governments to work closely with the private sector, often in Public-Private Partnerships (PPPs) to help manage the threats to these Critical Information Infrastructures (CIIs) and to work on solutions. The private sector is often the first to detect these threats, but government CERTs can also play a vital role in coordinating the response. Specific models of PPP have evolved to ensure this sharing of information is timely and effective, including the Information Sharing and Analysis Centre (ISAC) model developed in the United States nearly 20 years ago, the Information Exchange (IE) model and recently the Cybersecurity Information Sharing Partnership (CISP) both developed in the UK, and the Dutch ISAC variant, to name but a few.

Governments also need to talk to each other about these issues, both bilaterally, and sometimes in a government-only confidential forum where they can share experiences and solutions, and build networks of trusted international government contacts without commercial pressures from private sector partners. A global forum of this kind is provided uniquely by the series of Meridian Conferences which take place in a different country and region each year; the 11th annual conference will be held in Spain this October 2015, hosted by the Spanish CIIP agency CNPIC, and after the 2013 conference was hosted by Argentina, Meridian plans to return to the Americas in 2016.

The big issue of growing concern that brings together CIP and CIIP operators and governments is the crossover area known as Supervisory Control and Data Acquisition (SCADA) systems security, or Industrial Control Systems (ICS) security. These include the systems controlling flood defenses, dams, electricity generation installations, oil pipelines, chemical plant controls, and many other critical infrastructure components. Before this century these were often manual controls, or computer-controlled by obscure specialist hardware and software, understood by only a few engineers and specialists.

Every day now, more and more of these systems are becoming computerized with remote communications controls, and are almost always linked to the Internet somehow. That means that they have to be protected from some of the same malware and hacking exploits that can affect home or small business computer systems, and it means we are even more dependent on the resilience of the Internet. Just imagine a prolonged Internet outage that would not just take out your broadband, but your local water pumping station, the electricity generating system, the logistics center for delivery of raw ingredients to food factories and supermarkets, the oil delivery network supplying fuel to refineries and petrol to service stations—the nightmare is endless.

Fortunately there are many commercial organizations, private sector operators and government agencies working to ensure that critical information infrastructures are protected and resilient, and to make sure this nightmare doesn’t happen, and they are working in the best way possible – together.

United States Financial Services Information Sharing and Analysis Center (FS-ISAC)

The 2012-2013 DDoS attacks against the financial sector are an excellent example of coordinated sector response via the Financial Services Information Sharing and Analysis Center (FS-ISAC). Under the FS-ISAC All-Hazards Playbook, we stood up an incident action team comprised of 37 institutions that were being attacked. The sharing that happened amongst the group was phenomenal. We then took the information, aggregated and anonymized it and shared it with the rest of the sector partners such as the National Cybersecurity and Communications Integration Center (NCCIC) and other ISACs.

Information shared included indicators of compromise (IOCs), best practices, mitigation scripts, and strategies and lessons learned. We also worked very closely with the ISPs and mitigators and had meetings with them to share and develop best practices and mitigation strategies. The IAT also developed a threat viewpoint on DDoS that we updated three times as the tactics changed and shared with the sector and partners. The effort was so successful that the attackers went after other institutions as their tactics became less effective. On the last day of the last of 3 phases an institution who had not been attacked before was attacked but had no impact. They stated that because of the sharing that had happened previously they were able to put mitigation strategies in place which essentially thwarted the attack. This is an absolute example of information sharing at its finest.

Latin America and the Industrial Cybersecurity

The interest of the security community in analyzing and discovering new vulnerabilities in the industrial automation systems—especially the critical infrastructures—has grown rapidly. Even though this interest started in almost every important security conference back in 2013 and 2014, much has been said about the attacks on control and automation systems. There have been a great number of posts about this topic, as well as vendors adapting their technologies to provide "new" protection for these systems. More importantly there's the fact that the most prominent media have reported a significant number of attacks affecting mainly the production and distribution of oil, gas and energy.

Latin America has not been an exception—there's a great interest in investigating the potential weaknesses and the attacks carried out. The Latin American countries have been tracking such topics closely, even though they have lower budgets compared to those of the European countries and the United States.

By analyzing the three most representative countries in the region—Argentina, Brazil, and Colombia—we can observe three different ways to address the industrial cybersecurity, from totally different problems and particular characteristics of each country, which enrich them with their experiences in different ways.

In the case of Argentina, the "closed" definitions or the security multinational policies have not been directly enforced because the industrial systems implemented in the country are mostly (not all of them) outdated, hybrid or developed locally. Economic policy has driven the development of industrial control and monitoring systems, but the local developments can't always be applied to the same "policy package" created for other platforms. In this context, and based on the idea of open hardware projects such as Raspberry-Pi, Argentina has announced a project called CIAA, (Open Industrial Computer Argentina)[9]. This project aims to provide computers that can work in real-time to be used in industrial systems in small and medium-sized businesses (SMBs), since these businesses can't afford international brands, which are also scarce. Educational institutions such as universities can use these computers as well.

[9] http://www.proyecto-ciaa.com.ar

Regarding the political context around this topic, Argentina has created the National Program of Critical, Information and Cybersecurity Infrastructures[10], whose goal is "driving the creation and adoption of a specific regulatory framework that promote the identification and protection of strategic and critical infrastructures of the National Public Sector, inter-jurisdictional organizations, and civil and private organizations, and the collaboration of such sectors in order to develop appropriate strategies and structures to work together to implement a coordinated action by implementing the relevant technologies, among other actions".

This National Government program features tasks to substitute and monitor the critical infrastructures of the country. Unfortunately, public and private organizations joining the control framework set up by the ICIC is voluntary not mandatory, thus evolution is not as fast or agile as expected. However, with the support and conviction of those who support this topic, regular actions have been carried out, including industrial cybersecurity training for the representatives of the member companies, and also national exercises to respond to cyber incidents (ENRIC Program), and involving state stakeholders like the security authorities or the CERT.

On the other hand, Colombia was the first country in the region to take this topic seriously, and it has captured the world's attention. But even though this information could be surprising it isn't, because Colombia has been fighting against the Revolutionary Armed Forces of Colombia (FARC) for many decades, a fight that requires the Military Forces and the Police act in coordination with the private sector, to defend and protect the country's physical and virtual critical infrastructure. Thus, in the final stage of its National Policy of Cybersecurity and Cyber Defense (CONPES 3701/2011), work groups have been established and include National Government Institutions (Department of National Defense, MINTIC, National Police, etc.) and private organizations (representatives of the energy and communications sectors, administrators of the .co domains, universities, etc.) to create a very serious and coordinated framework to protect the critical infrastructures in the country.

Implementation will be led by the Colombia Computer Emergency Response Team (colCERT) with the aid of the Spanish private sector. ColCERT will identify, prioritize, and classify the country's critical infrastructure. It will serve as a cyberplatform that classifies critical infrastructure and interconnects national security organizations so they can provide effective protection. Finally, it will plan for and create a National Defense Strategy for Critical Infrastructure.

Brazil, the biggest country in Latin America, is also the most digitalized, and has the biggest investment in IT in the region. It is also the fourth country with the biggest number of Internet users in the world—there are more than 100 million people connected to Internet, driven by government incentives. The presidency of the Republic approved the Internet Civil Framework in April 2014, which lists rules, rights, and obligations for Internet use, as well as data protection.

The private and state organizations have included cybersecurity in their agenda since the preparation of the FIFA World Cup 2014, and they are getting prepared to host the 2016 Olympic Games in Rio de Janeiro. Events about SCADA and security have since been organized in that city.

According to different reports, Brazilian executives believe that most of the cybersecurity incidents are caused by hackers, competitors, cyber activists,

[10] www.icic.gob.ar

and current or former employees. The numbers of industrial security incidents is growing dramatically—the incidents in Brazil alone are rising in number, seriousness and sophistication. Since the hacktivism from LulzSec and LulzSecBrazil in 2014, the websites belonging to the Ministry of Sports, the Ministry of International Affairs, and the President's Office have been targeted with distributed denial-of-service (DDoS) attacks. Private information about public positions was also stolen. Because of the frequent news about corruption and social and political instability, we can expect a year full of cybersecurity incidents, especially industrial cybersecurity incidents.

"Data from Brazil, Chile, and Mexico reveals that most of the vulnerabilities are related to the wrong system configurations, followed by outdated versions and application problems."

In addition to the individual efforts of each country in the region, Peru and Chile, among other countries, have been doing a very interesting job in cybersecurity. Organizations like the Union of South American Nations (UNASUR)[11] and Member States have included cybersecurity and cyber defense in their agenda. They have also organized military conferences in different cities, and analyzed alliances and cooperation initiatives. However, beyond the work done by each country or by the organizations, there is no official information about security incidents in industrial systems or critical infrastructures in the region.

Incident evolution

Half of the companies in Latin America and the Caribbean were attacked in the recent years—not to mention government institutions, administrations and political organizations. The attacks keep on growing.

Argentina is one of the countries with the highest cybercrime activity in the world. Cyber threats in Colombia is high as well—almost half of the phishing attacks in Latin America occur in this country. These cyber attacks include fraud, targeted attacks, computer hijacking, hacktivism, public and private information and identity theft (especially in the finance sector), cyber terrorism and war, and military espionage. Cyber attacks in the region also include high-profile hacking and identity theft, similar to what happened with President Santos' email, that caused a major stir in the media.

On a global scale, two major trends in cybercrime are fraud with economic motivations, and attacks against confidentiality, integrity and availability.

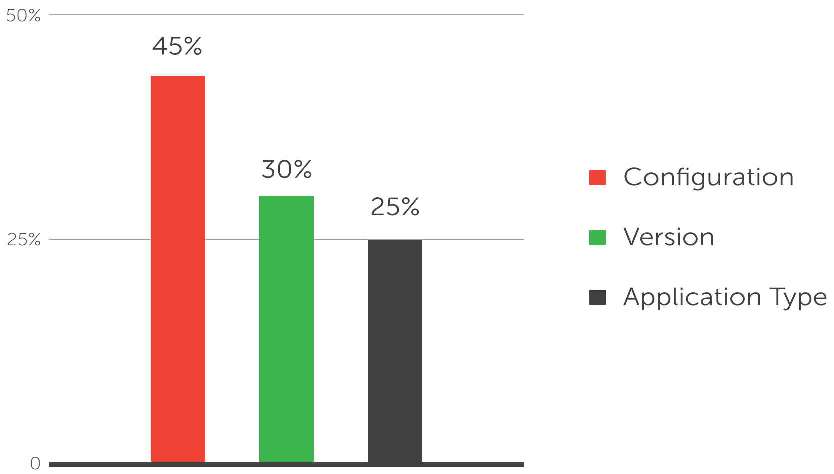
Vulnerabilities

The growth of targeted attacks, especially attacks that target sectors or infrastructures that provide critical services for the society and the State, drives the growth of the vulnerability detection services. This is done in order to help set priorities, fix security and compliances to prevent attacks, and facilitate the implementation of appropriate policies and strategies in each case.

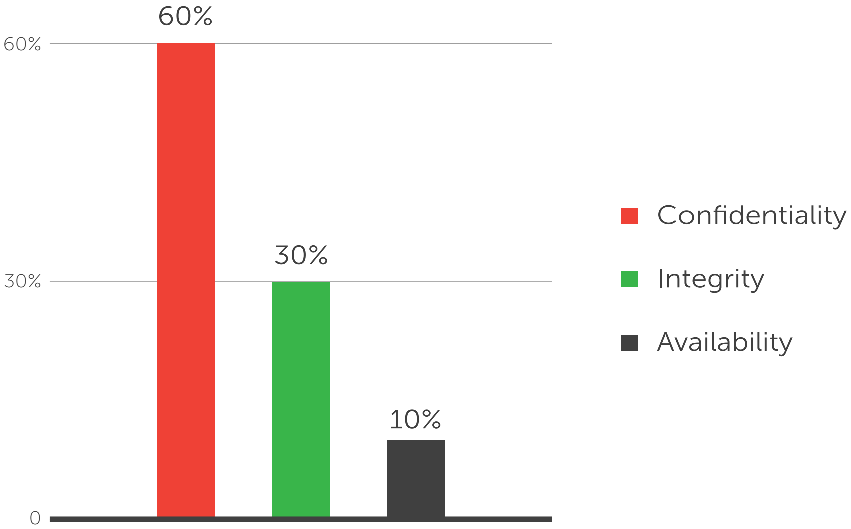
Data from Brazil, Chile, and Mexico reveals that most of the vulnerabilities are related to the wrong system configurations, followed by outdated versions and application problems. However, those problems are associated with a higher risk level.

60% of vulnerabilities that expose holes could affect information confidentiality. 30% of vulnerabilities represent a threat against integrity, while 10% of vulnerabilities are weaknesses that can take advantage of attacks against the availability of information and services.

[11] http://www.unasurs.org/node/13



Vulnerability types



Vulnerability reach

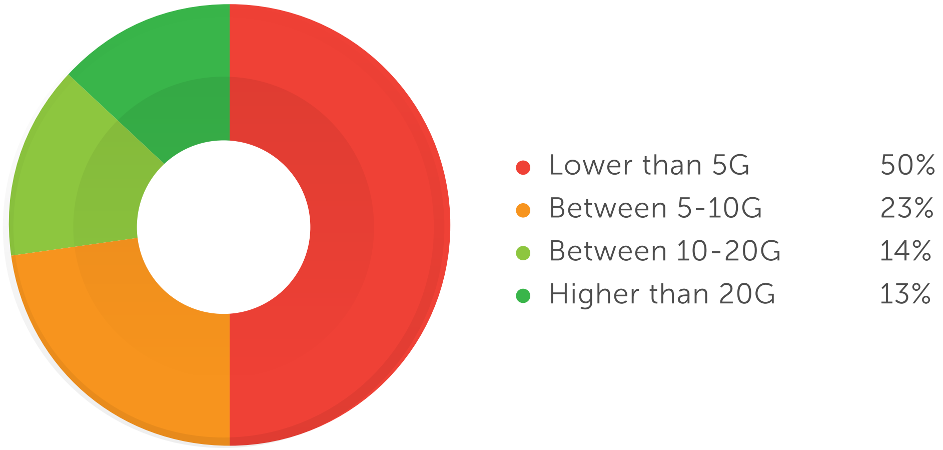
Distributed Denial of Service (DDoS)

The “DDoS-for-hire” attacks and the reflection and multi-vector attacks are a growing trend as regards the number and volume of incidents. These attacks’ victims include providers of finance services, e-commerce companies, government institutions, digital media, data centers, etc.

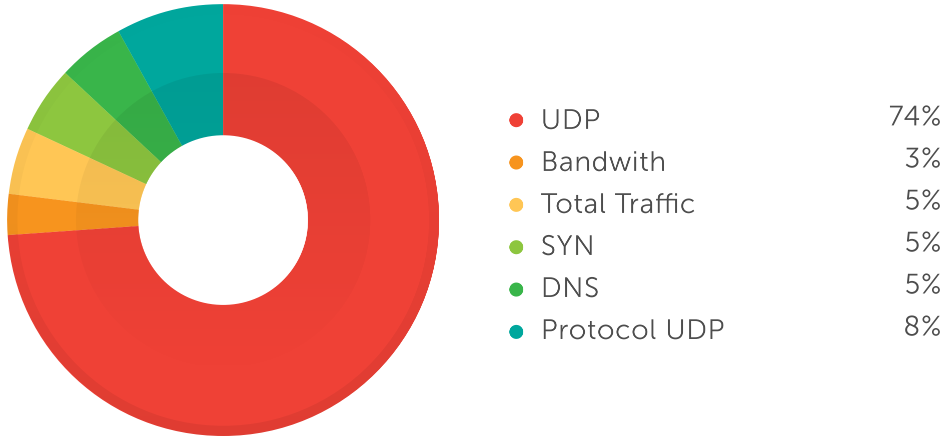
In Chile, a single victim suffered as much as 35 DDoS attacks in a month in 2014. 50% of the observed attacks had a bandwidth lower than 5Gbps; while 25% of the attacks had bandwidths between 5 to10Gbps; and the remaining 25% included incidents with volumes between 10 and 20Gbps. The most frequent attacks had bandwidths higher than 20Gbps. The 50Gbps attacks are increasingly common. The information is similar to the rest of the countries in the region.

Most of the attacks with a higher volume used the UDP protocol were targeted at NTP, DNS, SNMP, HTTP and HTTPS ports, which means a potential use of reflection/amplification mechanisms to create traffic.

A significant increase of the volume of attacks against SSL/TLS has been observed.



Types of UDP attacks: flood attacks using the UDP protocol.



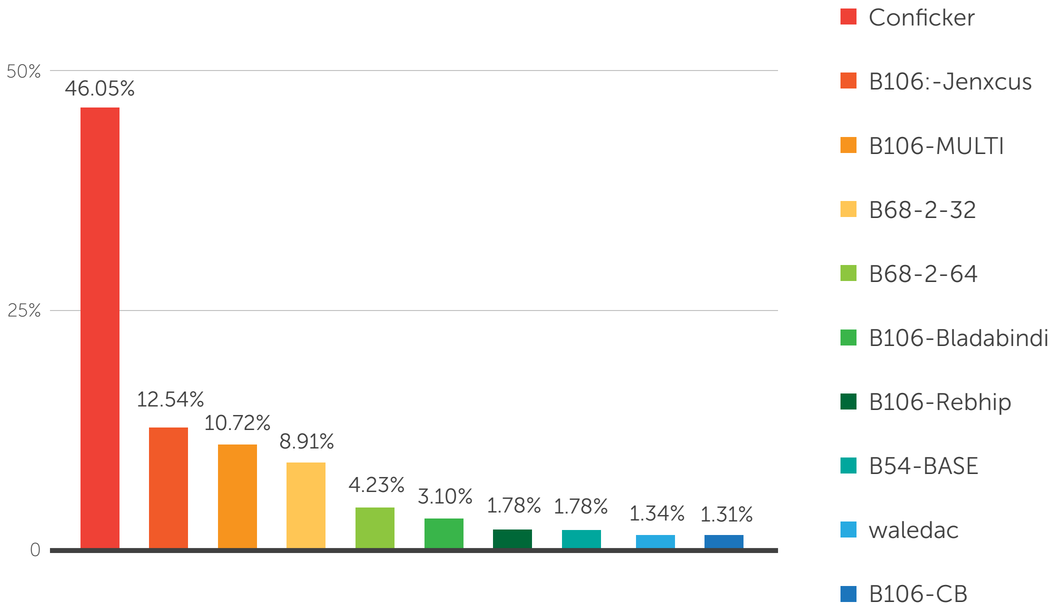
Types of UDP protocol attacks: Attacks using anomalies in the UDP protocol

Spam and malware

Confidential information theft remains the main motivation for those who use email to spread threats. Social media also remains the perfect target for this category of cybercrime.

Fraud against finance entities uses spam to hide phishing, malware and data theft. According to service and contents providers in Brazil, around two million spammed emails are managed per day, with a significant percentage of these emails mimicking credit card notices.

According to data about malware in the Spanish speaking region, around 1.5 million connection attempts from the infected machines to their respective C&Cs are reported each day. Around 10,000 different IPs per day are identified, and 7,000 different IPs per week are infected with malware, which correspond to the activity of around 50 different botnets, including DOWNAD/Conficker[12], ZACCESS/ZeroAccess[13] and the B106 malware family[14].



Data for top malware activity as of February 2015

***Conficker**: botnet worm; **B106**: Identity theft/finance fraud/privacy invasion; **B68**: ZeroAccess: advertising/click fraud; **B54**: **Citadel**: Identity theft/finance fraud; **Waledac**: Spam*

All these indicators point to consolidating the idea of cybersecurity as a general necessity for the high public and private management and the country's citizens in general.

Abilities and challenges

Argentina

The ITC sector in Argentina makes a significant contribution to the GDP, around 4.5% and growing; Argentina is the third country that supports this sector the most, together with Brazil and Mexico. The public and private sectors would have invested €7.4 billion in ITC in 2013.

Cybersecurity of critical infrastructures suffers from a limited collaboration between the public and private sectors, insufficient specific regulations, and better awareness among some professionals in the sector, for whom cybersecurity is just to protect their SCADA networks (First Awareness Conference for the Protection of Critical Infrastructure and Cybersecurity, October 2012).

[12] http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm_downad
[13] http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/rtkt_zaccess
[14] https://csirt.cesnet.cz/_media/cs/services/x4/botnet_b106.pdf

The most significant challenges are those related to decision making and the adoption of organizational measures, in addition to reinforce coordination in all the public organizations, and between these and the private sector.

Brazil

The GDP of the Brazilian ITC sector grew by 5.3% in 2013 compared to the previous year, the highest growth since 2008. ITC billing in Brazil is growing by around 30% to €103 billion in 2013. Most of the expense in R&D in Latin America is in Brazil. In addition, Brazil is the first country in Latin America, and the seventh in the world, that invest the most in ITC; investment reached €48.2 billion in 2013.

"Governments and enterprise should basically promote an all-level cybersecurity culture that fosters threat prevention. International and domestic collaboration between the public and private sectors play a key role in strengthening national cybersecurity frameworks."

Cybersecurity is one of the key priorities of the National Defense Strategy. This document is inclusive, and it doesn't just covers military matters but also the protection of Brazilian critical infrastructures of the space, ITC and nuclear industries, with the aspiration to reduce the dependence on other countries. Brazil has a wide network of early alert centers and response teams against security incidents.

The challenges that Brazil is facing can be classified in three categories: Budgets for research, development, and innovation (R&D&I); organization and control of current cybersecurity systems; and reduction of the dependence of foreign countries regarding supplies and acquisitions.

Colombia

The income of the Colombian ITC industry reached €14 billion euros in 2012, 6% of the GDP with an annual growth of 9%. The ITC industry created 110,000 direct jobs and it's growing faster than others. The investment in the ITC sector reached €5.9 billion euros in 2013, so Colombia is the fourth Latin American country after Brazil, Mexico and Argentina.

The cybersecurity plan will be the road map for the Administration and will be applied to the critical infrastructures and private sector; highlights include: double-defense structure and cybersecurity for external and internal threats, growth in the technology assets; review and hardening of the current regulatory framework; and reinforcement of intelligence abilities – technical and human.

Colombia faces key challenges: educational to promote and consolidate a cybersecurity culture in every field; regulatory to set up a clear framework customized for the country's reality and its critical assets, with abilities to verify compliance.

Conclusion

Governments and enterprise should basically promote an all-level cybersecurity culture that fosters threat prevention. International and domestic collaboration between the public and private sectors play a key role in strengthening national cybersecurity frameworks. It is necessary to put in more legislative and regulatory work if progress is expected. Information exchange and operational response should be decisive as well.

OAS Country Survey Results

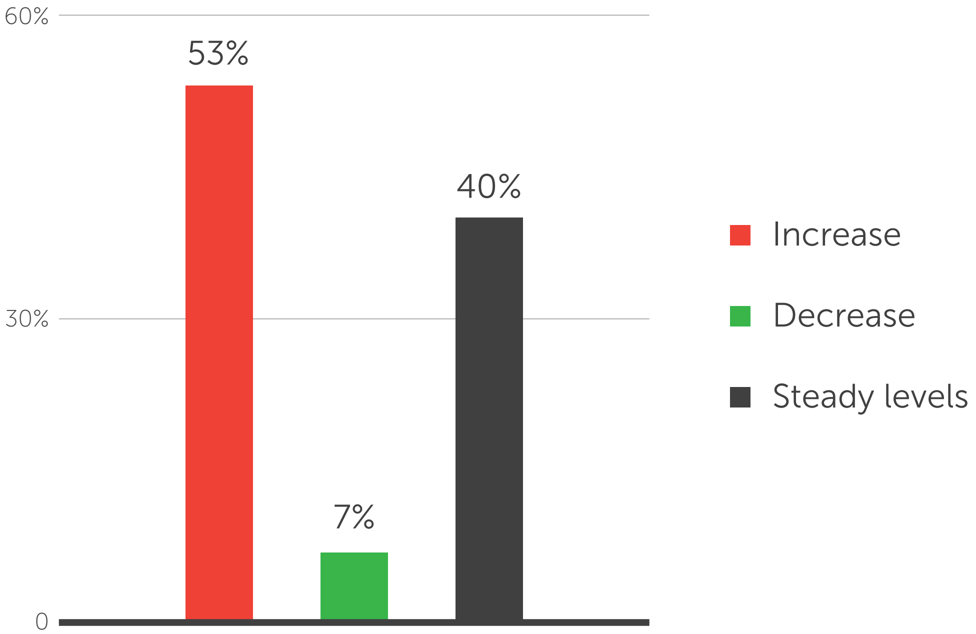
This section provides highlights and analyses of survey responses from Member States to questions around cybersecurity, attacks, preparedness and critical infrastructure.

An online quantitative survey was conducted by the OAS and Trend Micro in January 2015 among the Member States' Heads of Security of the major critical infrastructures in all countries in the Americas. Also included in this survey are private organizations who manage critical infrastructure within their countries. The survey is intended to give us a view of the state of critical infrastructure security within these Member States to help identify the strengths and weaknesses that need to be addressed.

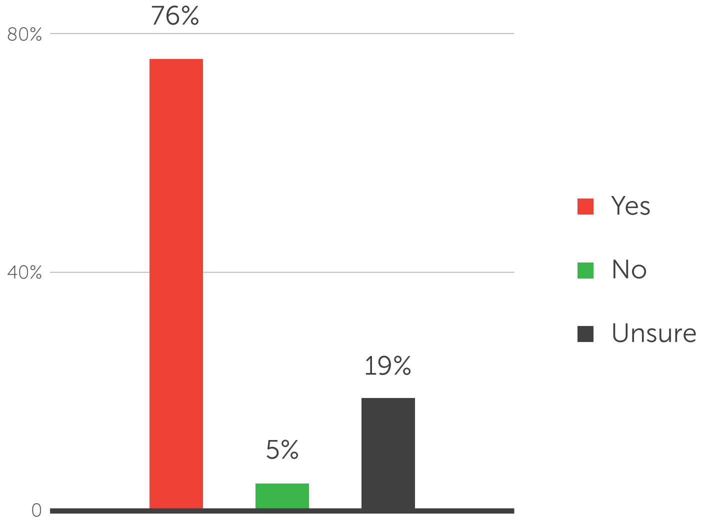
The first part of the survey assesses the state of the threat landscape within these regions and how prevalent and sophisticated the attacks being perpetrated.

Level of Incidents to the Computer System in the Last Year

Have you noticed an increase, decrease, or steady level of incidents to your computer systems in the last year?



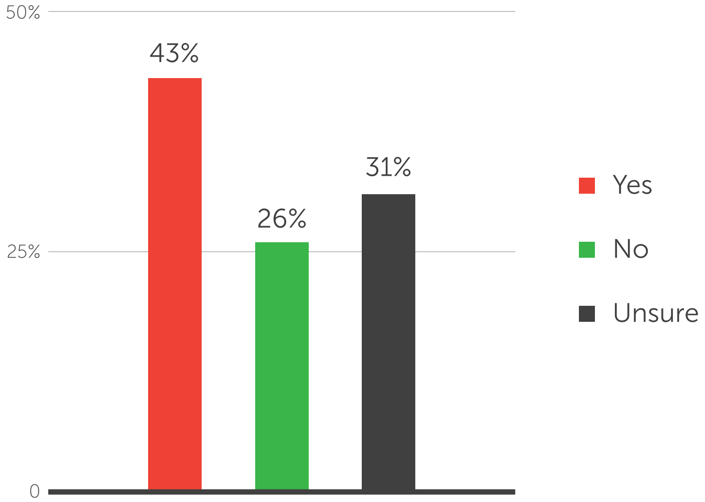
Are incidents against infrastructures getting more sophisticated?



The above results indicate that incidents are both increasing and getting more sophisticated as threat actors may target more vulnerable critical infrastructures in the future. These results would indicate a need to build better protections as well as improved incident response processes within regions to ensure effective mitigation of future attacks. With only 5% of the respondents stating attacks are not getting more sophisticated, this gives us insight into the threat actors' efforts at understanding how to compromise critical infrastructure and the need to improve their tools and techniques used in attacks. We are seeing a similar phenomenon with point-of-sale (PoS) system attacks that have occurred in the United States over the past year.

Attacks Targeting Infrastructure

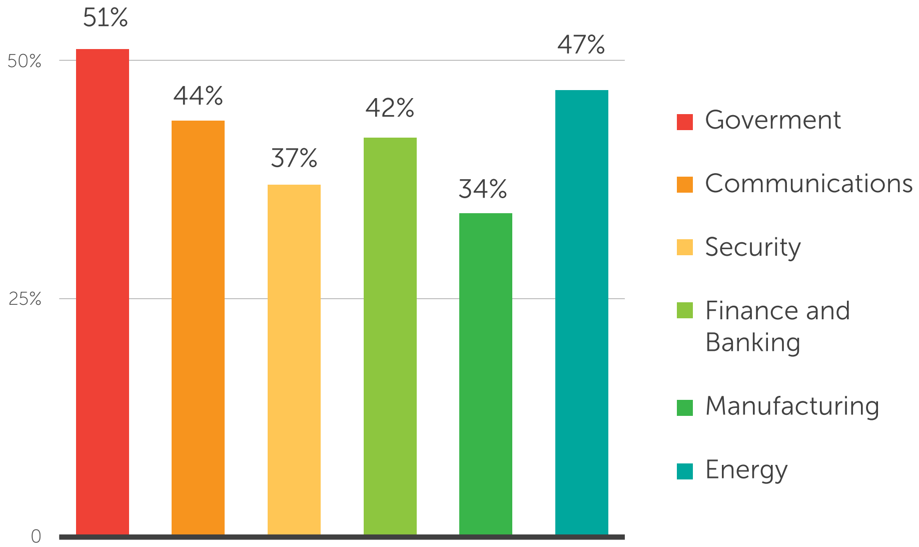
Have you detected any attacks/incidents/intrusions that were specifically targeting the infrastructure your organization operates/maintains/administers?



The data above shows a specific increase in critical infrastructure attacks (43%) with an alarming response of 31% that are unsure if they've been attacked. A major challenge today is the sophistication of attacks (76% say they are getting more sophisticated) which are difficult to detect. With almost a third of the respondents falling into this category, it is apparent that continuous monitoring controls are a needed requirement within most organizations to improve their visibility across their networks of attacker presence

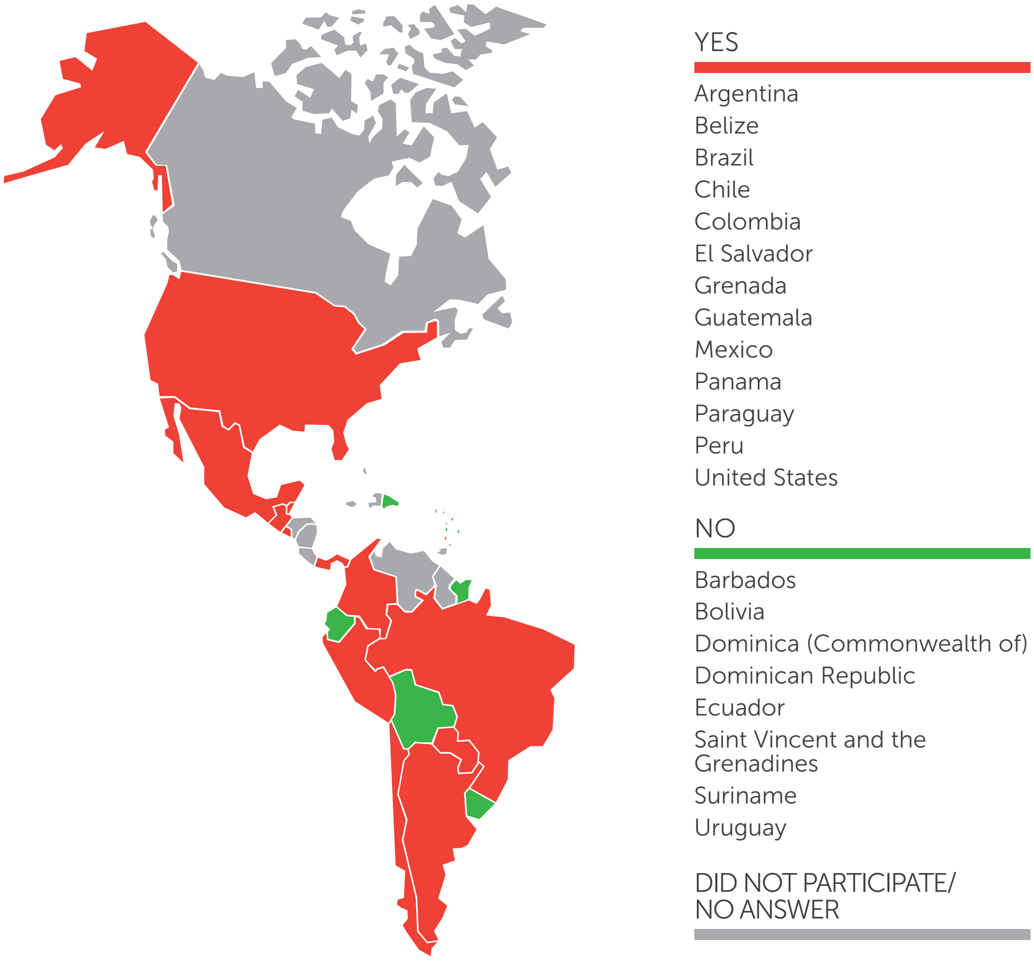
Experience with Various Incidents

Percentage of organizations that experienced attempts to have information deleted or destroyed by organization type



According to the survey results, the government and energy sectors are the top two industries that experience destructive attacks by threat, followed by communications and finance and banking.

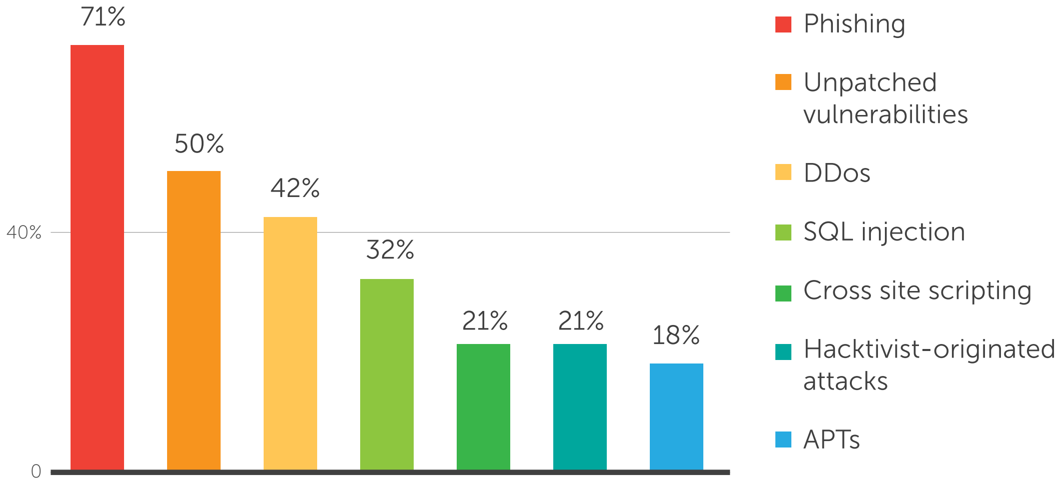
Government organizations that experienced attempts to manipulate organization’s equipment through a control network/system by country



The majority of regions surveyed indicated their ICS/SCADA equipment is being targeted by hackers, which indicate a broad amount of activity by threat actors. While many of these attacks may simply be gathering intelligence on their targets, we can expect to see more regions reporting this in the future as their critical infrastructures become more connected or gain an improved ability to identify an attack being present.

Types of Cyber Attack Methods

What types of cyber attack methods have been used against your organization?



From the above results we can see most regions are dealing with phishing attacks against their organizations.

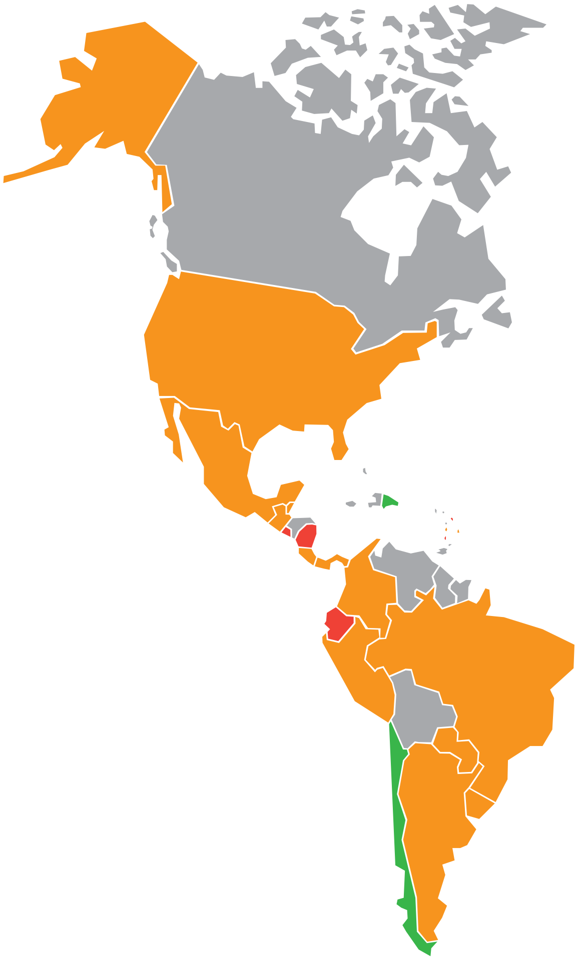
Phishing is the primary threat used in targeted attacks today and could be an indicator of the true state of targeted attack-related activities even though this was the lowest threat indicated in the results listed above. This may also indicate threat actors' initial attempts to penetrate an organization in an effort to move laterally across other systems, such as their ICS/SCADA devices.

Threat actors often utilize unpatched vulnerabilities in their attacks as they recognize patching is a difficult process for many organizations. Also, many critical infrastructure devices use older versions of operating systems and applications and are more prone to being vulnerable since many are out of support already.

As we've seen above, the attacks are getting more prevalent and sophisticated which will require organizations to be better prepared. Below we asked the regions to identify how prepared they currently are in the case of an attack.

Perception of Preparedness for Cyber Incidents

How prepared do you feel your organization is for a cyber incident?



NOT PREPARED 🟥

Dominica
Ecuador
El Salvador
Grenada
Nicaragua

SOMEWHAT PREPARED 🟧

Argentina
Barbados
Belize
Brazil
Colombia
Costa Rica
Guatemala
Mexico
Panama
Paraguay
Peru
Saint Vincent and the Grenadines
United States
Uruguay

PREPARED 🟩

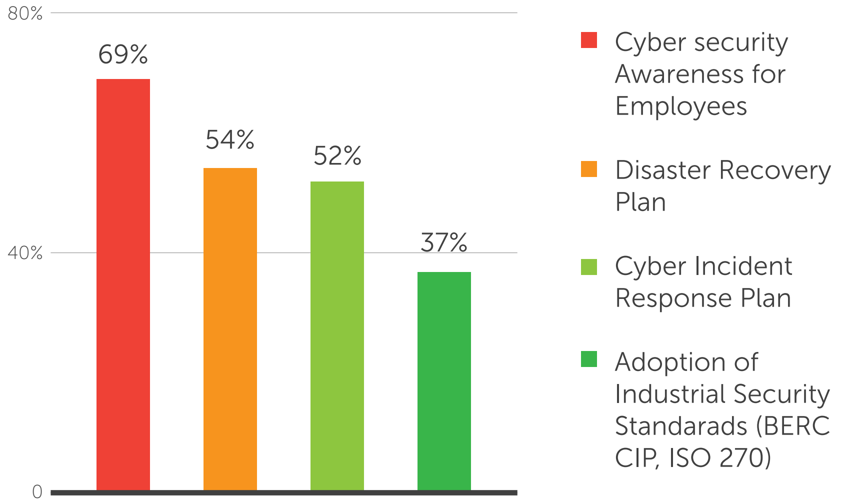
Chile
Dominican Republic

DID NOT PARTICIPATE/ NO ANSWER ▬

Most countries feel somewhat prepared for a cyber incident, which is good news, but the data in the succeeding survey results suggest that the efforts to improve preparedness may be more difficult than it appears. Also, the increase in the number and sophistication of attacks means that countries that are unprepared or somewhat prepared should immediately consider improving their detection, protection, and response capabilities.

Cybersecurity Policies

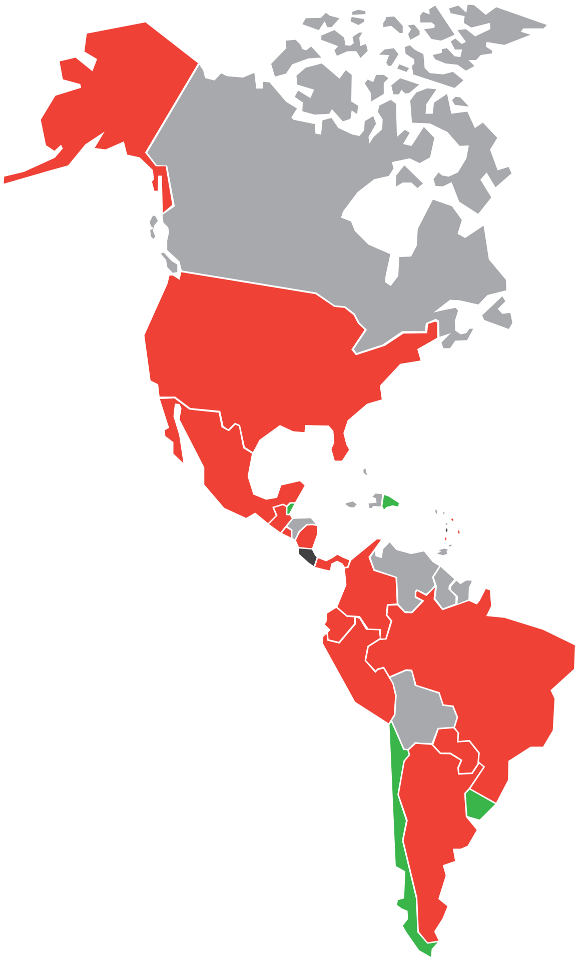
Does your organization have cybersecurity policies and/or plans?



Preparedness begins with having a plan and with just over half (52%) of the respondents stating they have a cyber incident response plan in place does not bode well should an attack occur. Industrial controls (ICS/SCADA) often have not been implemented with security measures in place and as such many regions have added regulations and standards for these. Only 37% of organizations have adopted those standards, which increase the risk of compromise for their devices.

Budget for Cybersecurity

Government organizations whose budget for cybersecurity increased over the last year



HAS NOT INCREASED 🟥

Argentina
Barbados
Brazil
Colombia
Dominica (Commonwealth of)
Ecuador
El Salvador
Grenada
Guatemala
Mexico
Nicaragua
Panama
Paraguay
Peru
United Sates

HAS INCREASED 🟩

Belize
Chile
Dominican Republic
Uruguay

UNSURE ⬛

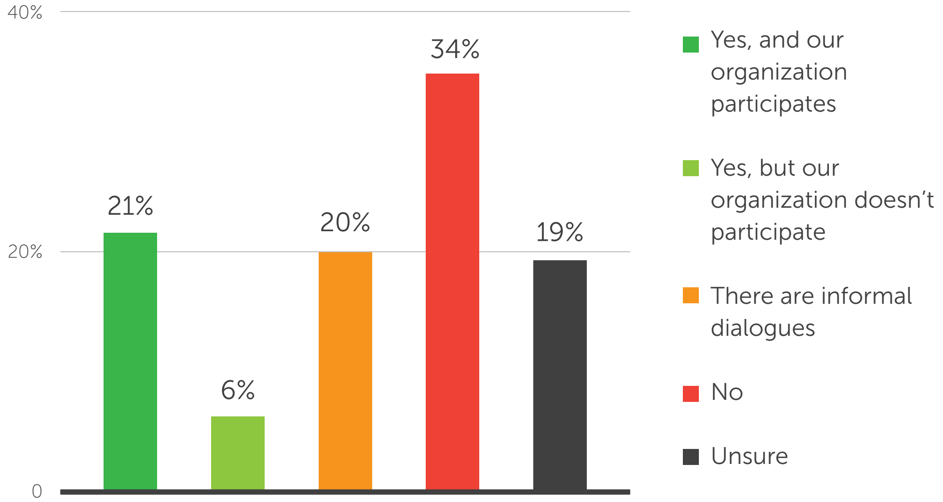
Costa Rica
Saint Vincent and the Grenadines

DID NOT PARTICIPATE/ NO ANSWER ⬜

With more than half of the respondents saying their budgets have not increased over the past year, the ability to detect intrusions will be severely compromised as most attacks today cannot be found using traditional security measures. Data breach detection systems can help improve this area, but we've seen these require additional budget to implement.

Discussion with Government about cyber resilience of Critical Infrastructure Systems

Is there a discussion/dialogue with government about the cyber resilience of critical infrastructure systems?

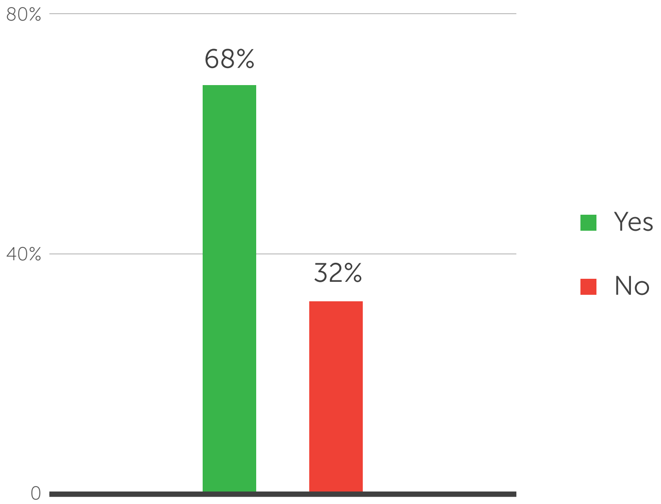


Since critical infrastructure affects everyone within a region, Public-Private Partnerships (PPPs) are key in properly managing the threat associated with threat actors looking to compromise these systems. With only 1 in 5 (21%) respondents stating an active dialogue there is a high level of improvement to be done to effectively deal with the threat.

If Respondents trust the Government to advance a Cybersecurity Agenda in Critical Infrastructure Industries

The good news is most respondents (68%) claim they trust their government to support advancements in dealing with the threat. This may indicate the barrier of implementing more dialogue is lower than it may seem and simply requires the public-private organizations to reach out to each other and start the process.

Do you trust the government to advance a cyber-security agenda in critical infrastructure industries? How willing are you to work with them?



Trend Micro Global Threat Intelligence Analysis

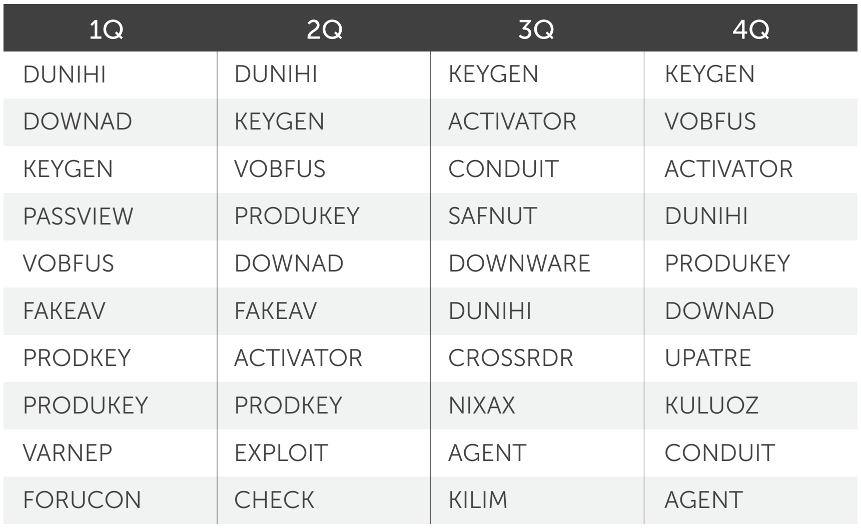
Malware

In 2014, the America region was affected by different malware, each with their distinct characteristics that could aid would-be attackers in their exploits. These range from worms (DUNIHI and DOWNAD/Conficker) to Trojans (AGENT and FAKEAV) to browser exploits (CONDUIT, SAFNUT, and CROSSRDR) to hacking tools/cracking applications (KEYGEN, ACTIVATOR, and PRODUKEY). As is observed in the last few years, insufficiently secured removable storage devices, unpatched operating systems (OSs) and/or applications, and indiscriminate user behavior online are some of the consistent factors that put users and organizations at risk to the evolving threats out there.

Top Malware Families for 2014

NAME	DESCRIPTION
KEYGEN	It generates serial numbers to crack into programs that need valid serial numbers for the programs to function fully.
DUNIHI	This malware family is commonly obfuscated VBS malware that is capable of propagating via removable drive infection; may arrive as an attachment to spam.
ACTIVATOR	This malware family cracks applications and may be manually installed by a user. It allows users to break the registration and protection techniques of applications, allowing them to use fully-registered version.
DOWNAD/Conficker	This exploits a vulnerability in server service that, when exploited, allows a remote user to execute arbitrary code on the infected system in order to propagate across networks.
CONDUIT	This malware family is bundled with malware packages as a malware component, or as a file dropped by other malware, or a file downloaded unknowingly by users when visiting malicious sites.
PRODUKEY	An application that displays the product ID and CD-Key of certain software if installed on the affected system. This hacking tool may be manually installed by a user.
SAFNUT	This malware family is bundled with malware packages as a malware component. It arrives in systems as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.
AGENT	It typically carries payloads or other malicious actions, ranging from mildly annoying to irreparably destructive ones. They may also modify system settings to automatically start. Restoring affected systems may require procedures other than scanning with an antivirus program.
CROSSRDR	This malware family is bundled with malware packages as a malware component. It arrives on a system as file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.
FAKEAV	This malware family creates folders on the affected system and drops various files, including a copy of itself and a malicious file. It makes several changes to the registry, one of which allows it to run at every system startup.

Top Malware Families in the Americas per Quarter



1Q	2Q	3Q	4Q
DUNIHI	DUNIHI	KEYGEN	KEYGEN
DOWNAD	KEYGEN	ACTIVATOR	VOBFUS
KEYGEN	VOBFUS	CONDUIT	ACTIVATOR
PASSVIEW	PRODUKEY	SAFNUT	DUNIHI
VOBFUS	DOWNAD	DOWNWARE	PRODUKEY
FAKEAV	FAKEAV	DUNIHI	DOWNAD
PRODKEY	ACTIVATOR	CROSSRDR	UPATRE
PRODUKEY	PRODKEY	NIXAX	KULUOZ
VARNEP	EXPLOIT	AGENT	CONDUIT
FORUCON	CHECK	KILIM	AGENT

Spam

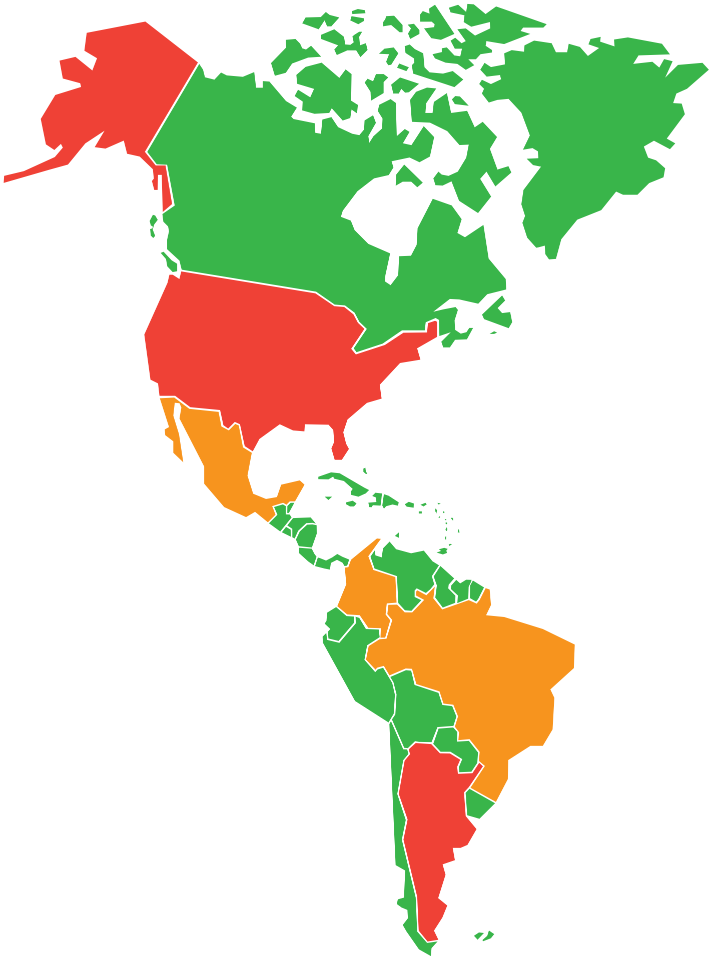
The global spam volume has seen an increase in the last couple of years.[15,16], The increase can be attributed to the prevalence of malware like the Trojan downloaders, which typically arrive in computers as attachments in email messages sent by spam botnets. Despite the increase in volume, email as an infection vector continues to decline. This may be because cybercriminals continue to explore and exploit other infection vectors like social networking sites and mobile devices.

As the data shows, among the countries in the Americas, the United States accounts for more than a quarter of the total spammed messages sent in 2014. Argentina follows close behind, while Colombia, Brazil, and Mexico top the list of spam-sending countries for 2014. These countries make up for more than 75% of the total number in the Americas.

[15] http://blog.trendmicro.com/trendlabs-security-intelligence/a-year-of-spam-the-notable-trends-of-2013/

[16] http://blog.trendmicro.com/trendlabs-security-intelligence/1h-2014-spam-attacks-and-trends/

Top Spam-sending Countries



> 20% 🟥

Argentina

United States

10-20% 🟧

Brazil

Mexico

Colombia

< 10% 🟩

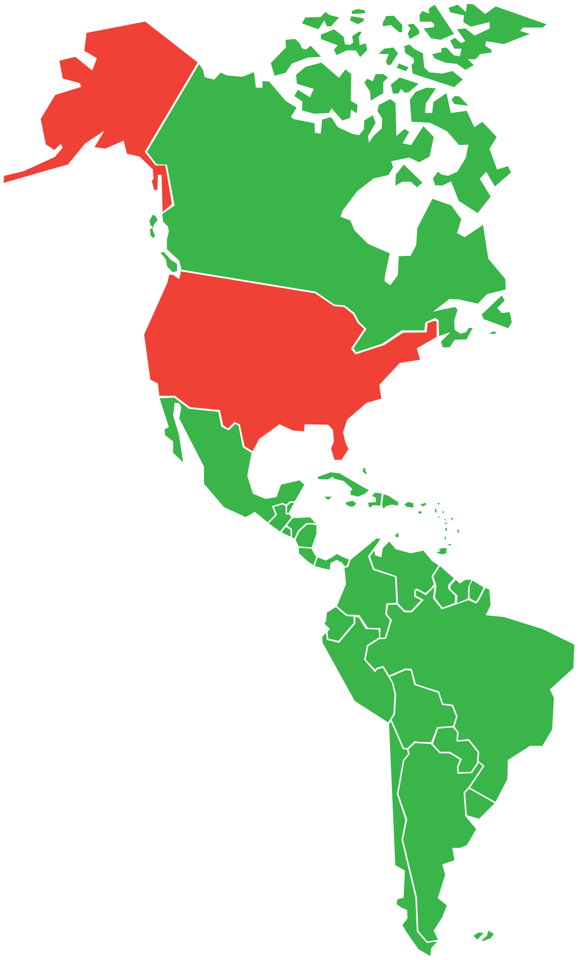
- Anguilla
- Antigua and Barbuda
- Aruba
- Bahamas
- Barbados
- Belize
- Bermuda
- Bolivia
- Canada
- Cayman Islands
- Chile
- Costa Rica
- Dominica
- Dominican Republic
- Ecuador
- El Salvador
- Falkland Islands
- French Guiana
- Greenland
- Grenada
- Guadaloupe
- Guatemala
- Guyana
- Haiti
- Honduras
- Jamaica
- Martinique
- Montserrat
- Nicaragua
- Nicaragua
- Panama
- Paraguay
- Peru
- Puerto rico
- Saint Kitts and Nevis
- Saint Lucia
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Suriname
- Trinidad and Tobago
- Turks and Caicos Islands
- Uruguay
- Venezuela
- British Virgin Islands
- US Virgin Islands

Malicious and Phishing Websites

Malicious websites, e.g., watering holes, hosted in the Americas continued to be an epidemic. Among the countries analyzed in this report, the United States not only topped the list, but also had the highest level of traffic to malicious sites. These malicious sites are categorized as disease vectors. These URLs are usually linked to spammed messages and may download other threats like malware on affected systems when accessed.

The United States also topped the other countries in the Americas in terms of phishing.

Top Phished Countries



> 20%

🟥

United States

< 10%

🟩

Brazil

Anguilla
Antigua and Barbuda
Argentina
Aruba
Bahamas
Barbados
Belize
Bolivia
Canada
Cayman Islands
Chile
Colombia
Cook Islands
Costa Rica
Cuba
Dominica
Dominican Republic
Ecuador
El Salvador
Falkland Islands Malvinas
French Guiana
Grenada
Guadeloupe
Guatemala
Guyana
Haiti

Honduras
Jamaica
Kiribati
Martinique
Mexico
Montserrat
Netherlands Antilles
Nicaragua
Panama
Paraguay
Peru
Puerto Rico
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
South Georgia and the South Sandwich Islands
Trinidad and Tobago
Turks and Caicos Islands
Uruguay
Venezuela
British Virgin Islands
US Virgin Islands

Underground Activity

Notable Threats and Threat Trends

The United States suffered from targeted attacks and PoS malware-related breaches. Retailers, banks, public utilities, and numerous organizations lost millions of customer data to attackers. More than monetary losses, the data breach incidents in the country caused huge brand and reputation damage to the organizations—in the case of Code Spaces, the damage was irreparable as they had to completely take down their site, which was brought about by their attacker deleting the site's client databases and backups.[17] P.F. Chang's had to go back to using manual credit-card-imprinting devices after a breach.[18] Target and Home Depot are the two largest data breach in the retail industry in terms of the number of payment card information stolen and litigation expenses. Before the year closed, America's most highly publicized targeted attack ensued: the Sony Pictures hack. The incident probably best showed how much a company could lose as an aftermath of a security breach—companies under the Sony banner have fallen victim to massive attacks. The company was forced to temporarily shut its network down after it was compromised by the so-called Guardians of Peace (GOP).[19]

Online banking theft, on the other hand, continued to be a serious problem in Latin America and the Caribbean, as cybercriminals continue to find new ways in infecting users and undermining the security measures. One example is the BANLOAD Trojan, a family of banking Trojans that targets Brazilian banking institutions.[20] In 2014, a BANLOAD variant was discovered to avoid detection and to limit its spread to other regions. This is done by checking specific security plugins first before attempting to perform its malicious routines.

Another tactic used to compromise user online banking credentials is the use of malicious control panel (CPL) files.[21] In terms of analysis, looking at a CPL file is essentially identical to a DLL file. However, unlike the latter, it is automatically run when double-clicked. This makes it similar to EXE files; however uneducated users may be more likely to try to execute CPL files if they do not know any better.

Malicious browser extensions have also been used to infect users in the region. Instead of running an executable file, users are prompted or are tricked into installing a malicious browser extension, which, if successfully installed, typically hijacks the victims' social networking accounts to spread a copy of itself.

[17] http://www.networkcomputing.com/cloud-infrastructure/code-spaces-a-lesson-in-cloud-backup/a/d-id/1279116

[18] http://www.usatoday.com/story/money/business/2014/08/04/pfchang-credit-debit-card-data-breach/13567795/

[19] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-magnified-losses-amplified-need-for-cyber-attack-preparedness.pdf

[20] http://blog.trendmicro.com/trendlabs-security-intelligence/banload-limits-targets-via-security-plugin/

[21] http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-cpl-malware/

Cybercriminal Underground in the Americas

Trend Micro continued to closely observe underground markets in different countries all over the world.[22] In 2014, Trend Micro researchers took a look at the Brazilian underground economy,[23] which appears to be continuously maturing despite lack of development in the tools and tactics they offer.

Some identified Cybercriminal underground markets possess unique characteristics. One of which is its use of popular social media platforms to commit fraud instead of hiding in the deep recesses of the Web with tools that ordinary users normally don’t have access to. Cybercriminals in these areas make use of popular mediums, such as social networks like Facebook, YouTube, Twitter, Skype, and WhatsApp, as these have turned out to be effective venues.

In some cases the underground Cybercriminals are players that market number generators and checkers or testers for more than just credit cards. They offer tools created for attacks against products and services exclusive in a particular country while also offering training services for cybercriminal wannabes. Among the products being offered, apart from banking Trojans, are account credentials for popular business applications, phishing pages, and phone number lists.

[22] http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/

[23] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-underground-market-for-cybercriminal-wannabes

Case Studies

Argentina

With over 32.9 million internet users—more than 76% of its total population—and more than 22 million units of PC equipment in the country, the Republic of Argentina finds itself among the top countries in the region in terms of adopting Information and Communication Technologies (ICT).[24] In addition, mobile connections including connected PCs and tablets, as well as smartphones and other cellular apparatuses with data service packages or free Wi-Fi have grown at an exponential rate, arriving at 20 million connections by the end of 2014. A significant component of this rapid growth has been a number of state policies and programs such as "Argentina Connected" and "Connect-Equality," which aim to increase broadband connectivity across the country and promote digital inclusion among public school students and teachers regardless of socioeconomic background. As Argentine society becomes increasingly connected to the Internet, it becomes imperative that citizens understand the risks associated with circulating "sensitive" information, such as identifiable characteristics, credit cards, bank statements and other personal information.

In addition to the growth of ICT in greater Argentine society, state government institutions have likewise digitalized much of their critical infrastructure. For example, the National Social Security Administration (Spanish acronym ANSES) and the Federal Administration of Public Revenue (Spanish acronym AFIP) have digitized much of their services. Furthermore, a great quantity of State procedures and transactions now occur over the Internet.

[24] Data provided by the "total market" study conducted by Prince Consulting, December 2014. www.princeconsulting.biz

Not only do these changes reflect government but also the private sector. Currently, there are 758 Internet service providers (ISP) in the country[25] and the mobile phone industry has quadrupled in size since 2003, when it overtook fixed lines, with 43 million active service lines. Such developments have increased the country's risk of being a target for cybercrime or other malicious criminal activities; over the past year, national authorities have observed increases in identity theft and fraud via social networks, e-mail or e-banking, website defacements and targeted attacks.[26]

In order to address these cyber threats, in 2011 the National Government, through the Chief of the Cabinet of Ministers, created the National Information Critical Infrastructure and Cybersecurity Program (known as the acronym ICIC). The ICIC is designed to support the creation and adoption of a specific regulatory framework aimed at identifying and protecting strategic and critical infrastructures as needed by the National Public Sector, inter-jurisdictional organizations, civil society and the private sector.

Among others, the objectives developed by ICIC are:

- To sensitize citizens and organizations to the risks that new technologies hold and to encourage them to protect their information.
- To strengthen cybersecurity levels in the National Public Sector, creating common strategies for protecting information and critical infrastructures.
- To encourage collaboration among different sectors of society (businesses, industries, civil society organizations, universities, etc.) with the aim of adopting a common framework of guidelines for strengthening their organizations' levels of cybersecurity and critical information infrastructures.
- To contribute internationally to the improvement of cybersecurity and critical information infrastructure.

As of 2014, ICIC has accomplished the following:[27]

- Helped pass the current cybercrime-related legislation, which has allowed for the successful investigation and prosecution of several cyber-criminal cases.
- Developed the initiative known as Internet Sano ("healthy" or "sound" internet), which promotes and provides educational material on responsible ICT and internet use.
- Since 2012, carried out annual cyber incident response exercises – called ENRIC – and continues to provide training in identifying, analyzing, preventing, strengthening, recuperating and responding to incidents involving information infrastructure

> *"Currently, there are 758 Internet service providers (ISP) in the country and the mobile phone industry has quadrupled in size since 2003, when it overtook fixed lines, with 43 million active service lines. Such developments have increased the country's risk of being a target for cybercrime or other malicious criminal activities; over the past year, national authorities have observed increases in identity theft and fraud via social networks, e-mail or e-banking, website defacements and targeted attacks."*

[25] Source: Comisión Nacional de Comunicaciones http://www.cnc.gob.ar/

[26] Source: Organization of American States, *Latin American + Caribbean Cybersecurity Trends*, June, 2014.

[27] Source: Organization of American States, *Latin American + Caribbean Cybersecurity Trends*, June, 2014.

Since 2011, the ICIC has partnered with various national and international organizations and has likely influenced a greater interest within Argentina in addressing cybersecurity issues. The ICIC has actively participated in events sponsored by OAS, European Union Institute for Security Studies (EUISS), International Atomic Energy Agency (IAEA), Meridian Process, among others. Also, several institutions of higher learning in the country now offer certification and degree programs in many cybersecurity-related fields, including digital forensics.

Although Argentina's capacity for handling cyber threats has shown great improvement since ICIC's founding, an OAS report highlighted three main impediments to on-going efforts that still exist: the persistent lack of awareness among stakeholders at all levels, issues and concerns regarding privacy, and insufficient funding. Such challenges will need to be addressed going forward to ensure the success of Argentina's cybersecurity efforts.

Trinidad and Tobago

Accounting for over forty percent (40%) of the country's gross domestic product (GDP), the energy sector is the primary income earner in Trinidad and Tobago. As a result, the components of this sector are regarded as critical infrastructure resources. From programmable logic controllers (PLC) to control networks such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA); there is pervasive use of information and communication technologies (ICTs) throughout the energy sector in Trinidad and Tobago that make it vulnerable to cyber-related threats. Disruptions arising from these vulnerabilities can potentially have a crippling effect on the national economy.

It is important to note also that critical infrastructure components for Trinidad and Tobago may be found in other sectors including finance, telecommunications, public utilities and health. However, like energy, the finance sector has particular significance in terms of cybersecurity and critical infrastructure protection (CIP), as attacks on any one institution within this sector can have a debilitating effect on the entire financial sector.

In recognition of the need for the protection of critical infrastructure through the development of a robust cybersecurity framework, the Government of Trinidad and Tobago, in 2011, established an Inter-Ministerial Committee (IMC) to develop a comprehensive cybersecurity strategy for Trinidad and Tobago. Comprising various key Ministries (including the Ministries of Science and Technology, Public Administration, the Attorney General, Public Utilities, Finance, Energy and Energy Affairs), the IMC was mandated to, *inter alia*:

- Develop a coordinated cybersecurity strategy and action plan
- Facilitate, guide and ensure the enactment of a national Cybercrime Act
- Facilitate, guide and ensure the implementation of a National Computer Security Incident Response Team (CSIRT)
- Establish an implementation mechanism that would have legislative authority to develop and enforce cybersecurity regulations
- Create a mechanism/framework that ensures that risk/vulnerability assessments of each Ministry's cyber infrastructure and cybersecurity plan are conducted regularly.

To date, the IMC has accomplished the following:

- Development of a National Cybersecurity Strategy (approved December, 2012)
- Development of a National Cybercrime Policy (approved February, 2013)
- Development of a Policy for the Establishment of a Trinidad and Tobago Cybersecurity Agency (approved August, 2013)
- Administrative Agreement between the Ministry of National Security and the International Telecommunication Union (ITU) for assistance in establishing a Computer Security Incident Response Team (CSIRT) (February, 2014)
- Drafted and obtained approval for the Bills entitled "The Cyber Crime Bill 2014" and "the Trinidad and Tobago Cybersecurity Agency Bill, 2014". The Cybercrime Bill was tabled in Parliament on Friday 21 March, 2014.

In addition to the overarching National Cybersecurity strategy which caters to the needs of both public and private stakeholders, the government has also established an Energy Sector Security Initiative (ESSI), which is aimed at providing strategic direction for the security and safety of Trinidad and Tobago's energy sector. The ESSI is a Public Private Partnership. It was formed via collaboration between the Government of Trinidad and Tobago and public and private sector owners and operators of key energy infrastructure. The principal focus of the Initiative is to create a sustainable mechanism to prevent, mitigate, prepare for, respond to and recover from all possible threats and vulnerabilities which have the potential to disrupt or destroy Trinidad and Tobago's energy sector.

The strategic objective of the ESSI is the prevention and mitigation of any unwanted occurrences within the energy sector. As such, the Initiative is intended to ensure that Trinidad and Tobago's energy-based resources and assets are effectively protected against activities that could result in major disruptions occasioned through willful intent, accidents or natural disasters.

Uruguay

The Eastern Republic of Uruguay has seen the increasing development of Information and Communication Technology (ICT) at the national level. Perhaps not surprisingly, data suggests that cyber incidents, especially phishing, have significantly increased as well. Such threats carry serious ramifications for State critical information assets, i.e., those that are understood to be vital to government and economic operations, such as emergency services, health services, public order, energy, telecommunications, transport, potable water supply, banks and financial services or any other service that affects more than 30% of the population, and thus the security and well-being of greater society.

> *"Since its creation, CERTuy has coordinated and implemented response to an analysis of security incidents, supported and coordinated recovery processes from disasters, carried out penetration tests and security audits"*

In 2008, under the National Agency for the Development of e-Government and the Information Society (AGESIC), the National Cybersecurity Incidence Response Center was constituted by law (CERTuy). Since its creation, CERTuy has coordinated and implemented response to an analysis of security incidents, supported and coordinated recovery processes from disasters, carried out penetration tests and security audits. Also, it has developed and diffused norms, policies and best practices that increase levels of security. It has also worked forcefully in the development of capacity and the diffusion of knowledge through awareness-raising campaigns, capacity building for critical infrastructure operators through cyber crisis management exercises and specifically in the creation of specialized CSIRTs. CERTuy's objectives and mandates include:

- To promote trust among ICT users and raise greater society's awareness of cyber threats.
- To regulate and protect State critical information assets.
- To consolidate all critical national public service organizations under a common criteria for web-site classification (i.e. ".gub.uy" and ".mil.uy") and improve security standards for databases, email and domain names.
- To incorporate a multi-stakeholder approach among key national and regional actors (Judiciary, law enforcement, Ministry of National Defense, private and financial sectors, academia, internet service providers, civil society, CCIRTs and international organizations, among others).

Since its inception, CERTuy has accomplished the following:

- Detected intrusions of varying complexity and severity to critical systems that were able to be contained without generating greater impact.
- In cases of cyber incidents, offered rapid and effective responses in order to determine the systems affected and brought about efficient recovery efforts, which were achieved by incorporating incident-management methodologies, information-security specialist intervention, linking with various security actors, networks of national and international trust and the constant development of specific capacities.
- Announced in November 2013 the beginning of the "Connect Yourself Securely" campaign, which aims to raise public awareness of the threats that accompany the use of ICTs, as well as adopted the U.S.-founded STOP. THINK. CONNECT. campaign.
- Provided technical training to personnel from various counter cybercrime authorities, including the Computer Crime Unit of the National Police.

As aforementioned, CERTuy understands that alliances and the involvement of all cybersecurity actors, both public and private, are fundamental to be able to counteract the growing quantity and sophistication of threats to cybersecurity. Therefore, AGESIC and CERTuy have regularly coordinated efforts with counterpart authorities in other countries and partnered with international organizations working to foster communication and collaboration among response centers, such as OAS/CICTE, LACNIC, FIRST and ITU.

Uruguay's future success in combating cybercrime and other threats to cybersecurity will depend, in part, on its ability to address three main issues that have hampered progress: lagging cybersecurity awareness within other government institutions, insufficient financial and material resources to carry out needed initiatives, and a lack of trained personnel.[28] Nevertheless, CERTuy has continued to work arduously, continuously and collaboratively to protect Uruguay's critical infrastructure from cyber threats and to contribute to cybersecurity at the international level.

[28] Source: Organization of American States, *Latin American + Caribbean Cybers ecurity Trends, June 2014.*

Conclusion

This seminal report provides a unique perspective into the cyber attacks experienced by critical infrastructures in the Americas. The 500 respondents emphasized a dramatic increase in the sophistication of cyber attacks. Most troubling, was the ominous phenomenon depicted by the dramatic increase in destructive attacks—cyber attacks, which were intended to "delete or destroy" backend systems. There exists a clear and present danger, one which illustrates the dramatic evolution of cyber capabilities possessed by non-state actors groups in the region. These groups have adopted cyber attacks against infrastructures for the purposes of crime; activism and geopolitics. Given this stark reality, budgets for cybersecurity and capacity building must be increased and greater information sharing must be facilitated.

In conclusion, this report highlights that although some efforts have been made, there is still a lack of proactive partnership between governments and private organizations in the western hemisphere. In the absence of a formal public-private partnership these cybercriminals will thrive. This represents a historic missed opportunity. The OAS/CICTE Cybersecurity Program serves a pivotal role in fostering the public-private partnership that is still maturing in the region. It is in the spirit of such a public-private partnership that OAS and Trend Micro joined forces to provide you with this unique perspective into critical infrastructure attacks that have impacted 25 nations. Collective action is direly needed.

"Not all the armies of the history of the world can stop an idea whose time has come." –Victor Hugo

Appendix: Critical Infrastructure Survey

Methodology

- An online quantitative survey was conducted in January 2015 among the heads of Security of CIOs of the major critical infrastructures in all countries in the Americas.
- A total of 575 respondents completed the survey.

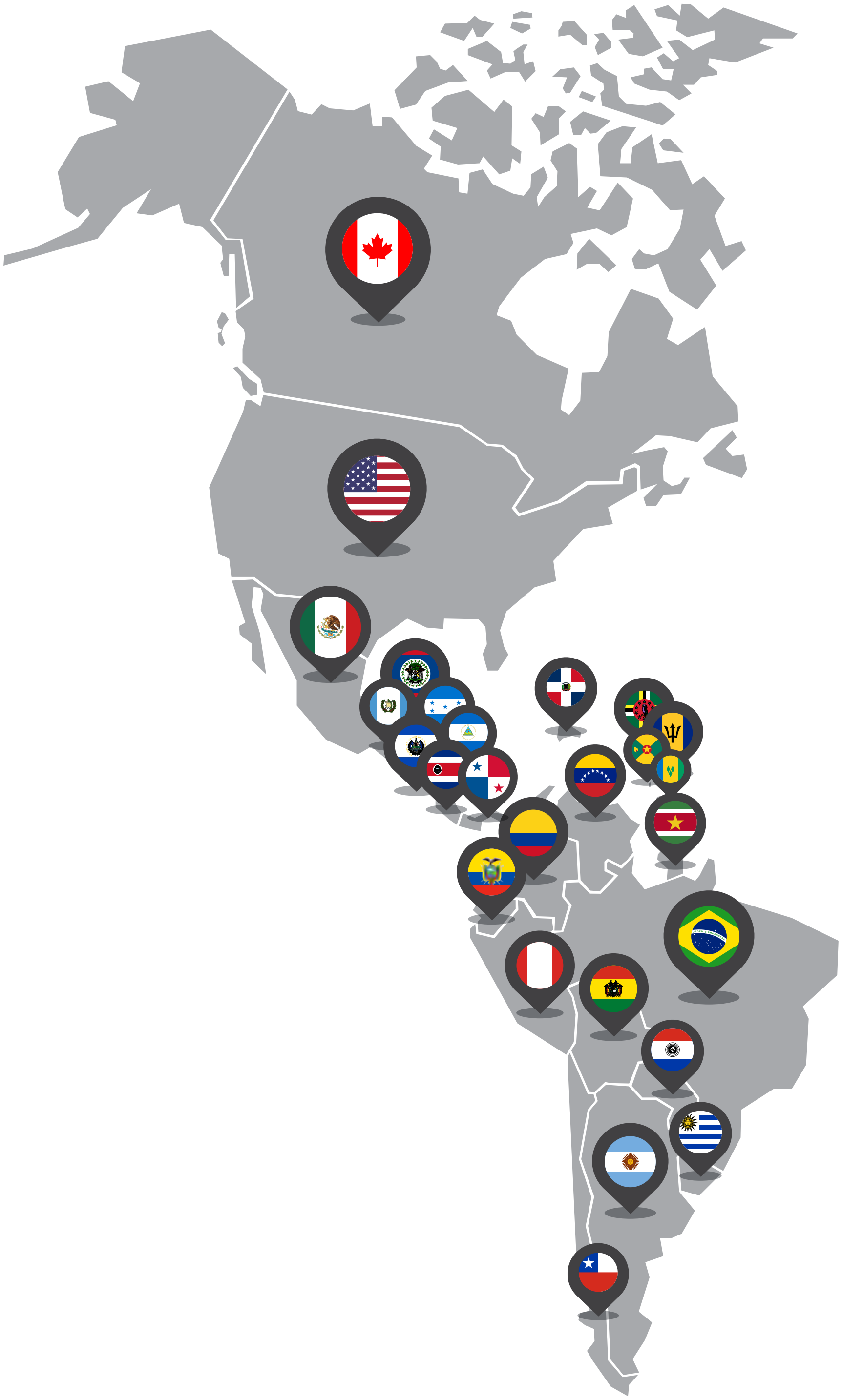
Survey Results

Respondent Countries

A total of 26 OAS member countries participated in the survey. They are:

- Argentina
- Barbados
- Belize
- Bolivia
- Brazil
- Canada
- Chile
- Colombia
- Costa Rica
- Dominica (Commonwealth of)
- Dominican Republic
- Ecuador
- El Salvador
- Grenada
- Guatemala
- Honduras
- Mexico
- Nicaragua
- Panama
- Paraguay
- Peru
- Saint Vincent and the Grenadines
- Suriname
- United States of America
- Uruguay
- Venezuela (Bolivarian Republic of)

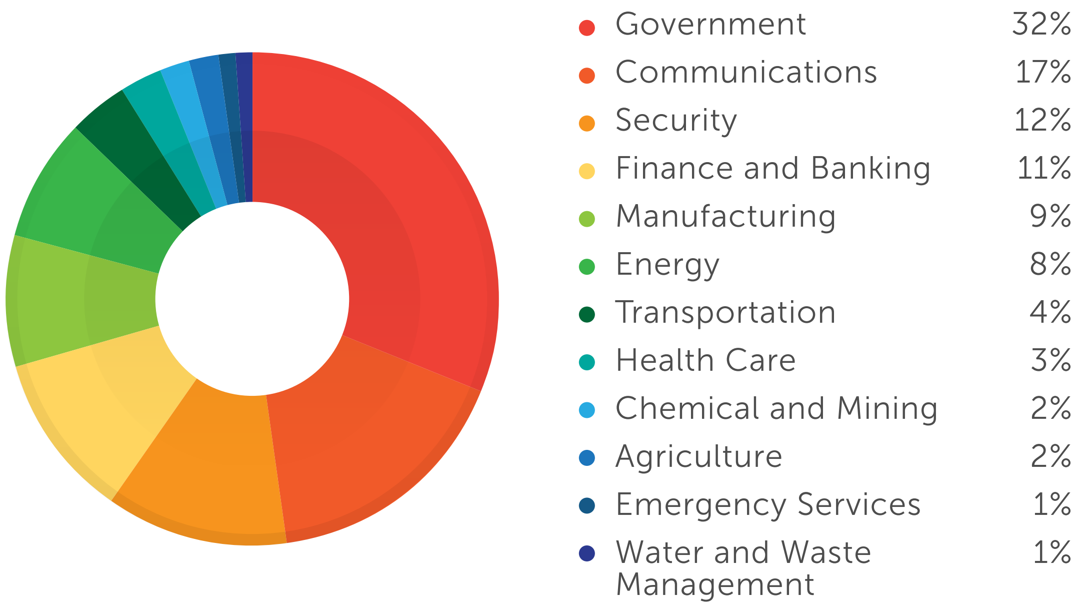
In what country do you currently work?



Organization Vertical

- The most commonly reported industry is government, followed by communications.

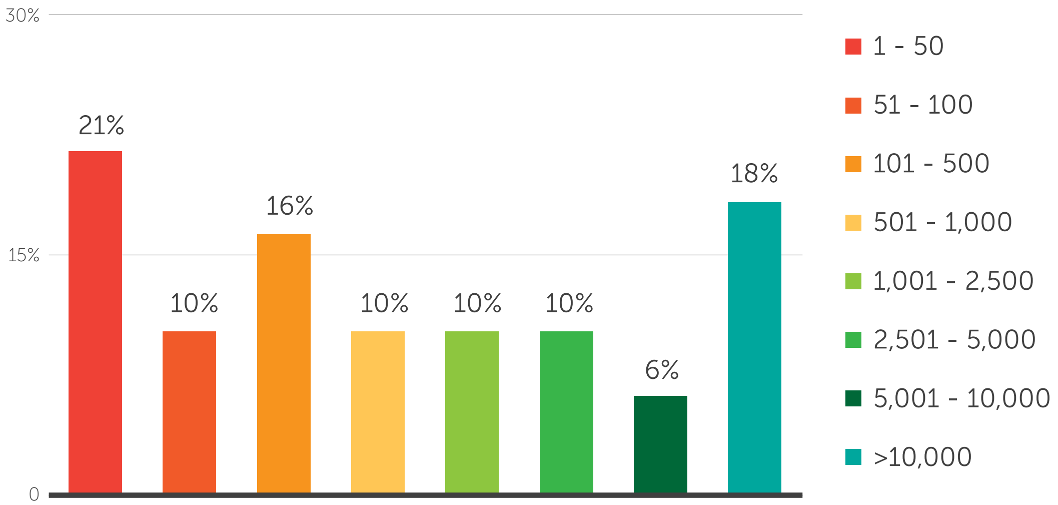
To which industry does your organization belong?



Organization Size

- Overall the organizations surveyed are spread across various org sizes. The two organization size groups that have the largest number of organizations are: “1-50 employees” (21%) and “> 10,000 employees” (18%).

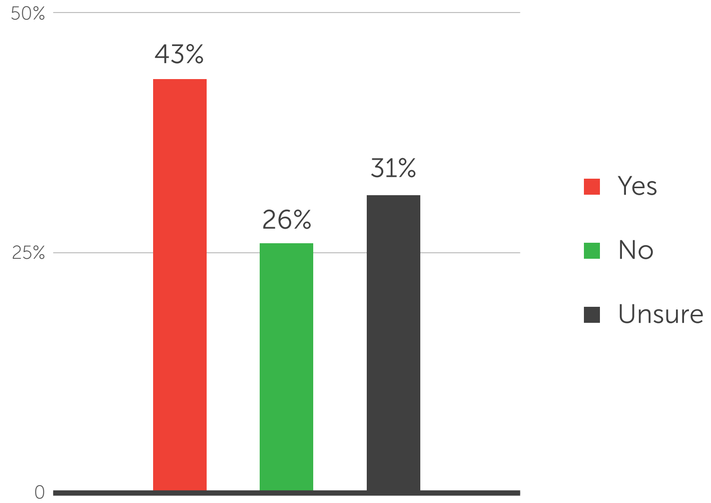
How many people does your organization employ worldwide?



Level of Incidents to the Computer System in the Last Year

- More than half of the respondents reported an increase in the level of incidents to their computer system in the last year, whilst 4 in 10 said the level of incidents was steady.
- Very few reported a decline in the level of incidents in the past year.

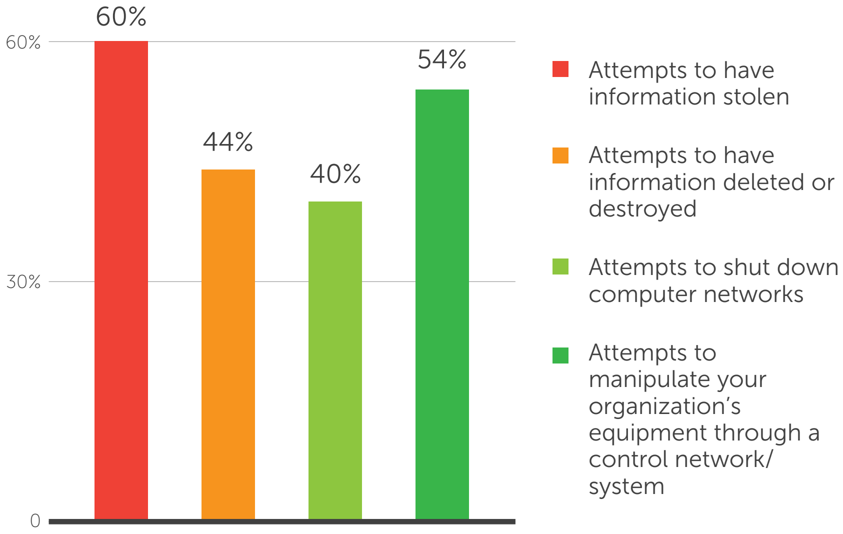
Have you noticed an increase, decrease, or steady level of incidents to your computer systems in the last year?



Experiences with Various Incidents

- Overall the majority of the organizations surveyed have experienced attempts to have their information stolen. More than half have experienced attempts to manipulate equipment through a control network/system.

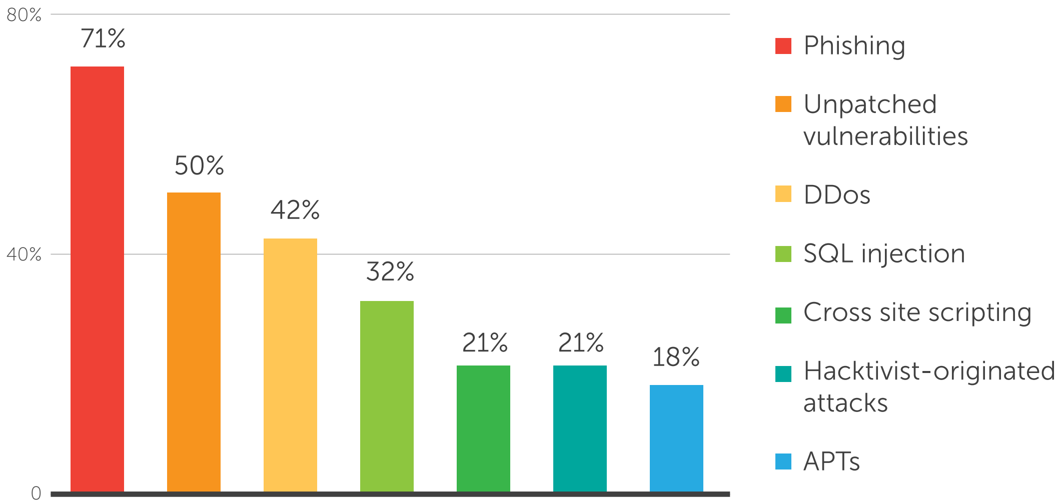
Has your organization experienced any of the following?



Types of Cyber Attack Methods

- The vast majority of the organizations reported phishing has been used against their organizations. Half reported unpatched vulnerabilities have been used against their organization.

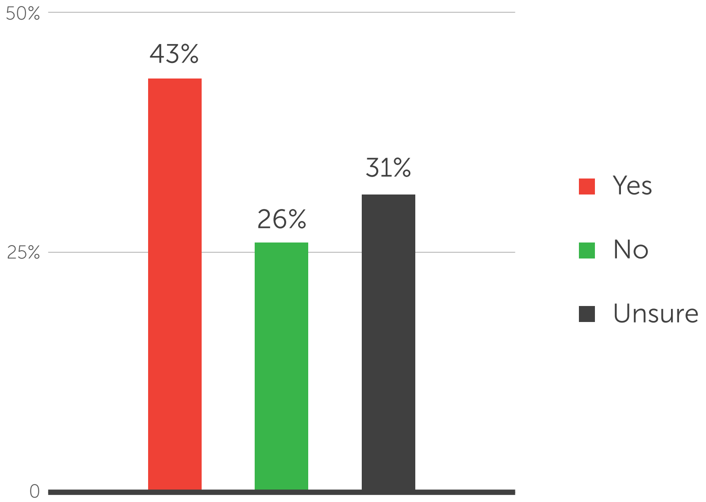
What types of cyber attack methods have been used against your organization?



Attacks Targeting Infrastructure

- More than four in 10 organizations have detected attacks that were specifically targeting the infrastructure they operate. Another three in 10 said they were not sure.

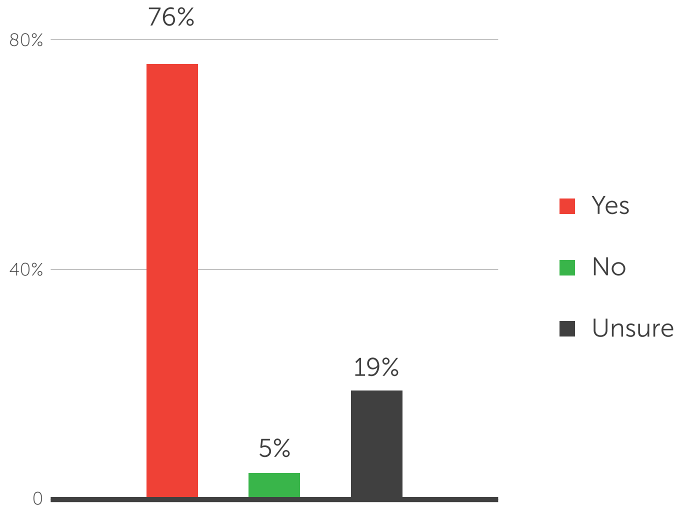
Have you detected any attacks/incidents/intrusions that were specifically targeting the infrastructure your organization operates/maintains/administers?



Sophistication of Attacks

- There is a universal consensus that the attacks against Infrastructure are getting more sophisticated in all countries surveyed.

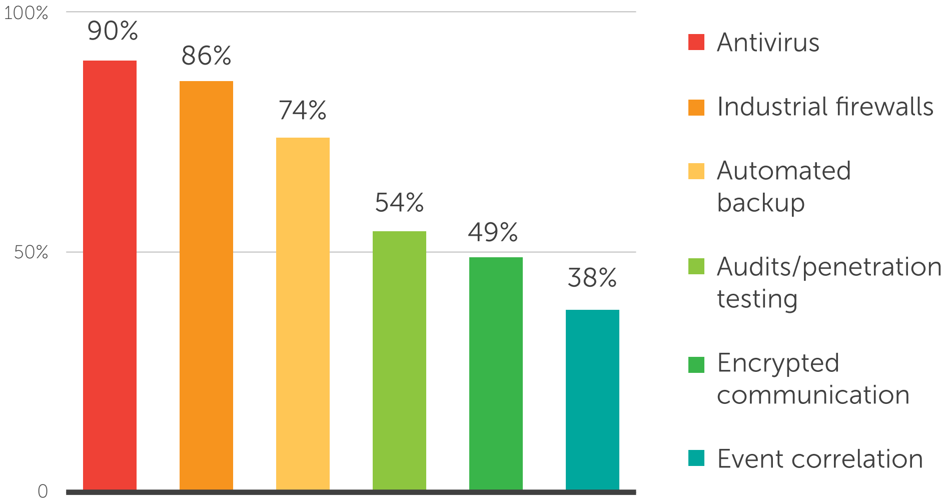
Are attacks against infrastructures getting more sophisticated?



Measures Taken To Protect Critical Information Systems

- Organizations used a variety of cybersecurity controls to protect critical information systems, the most common measures being deployed were: antivirus, industrial firewalls and automated backup.

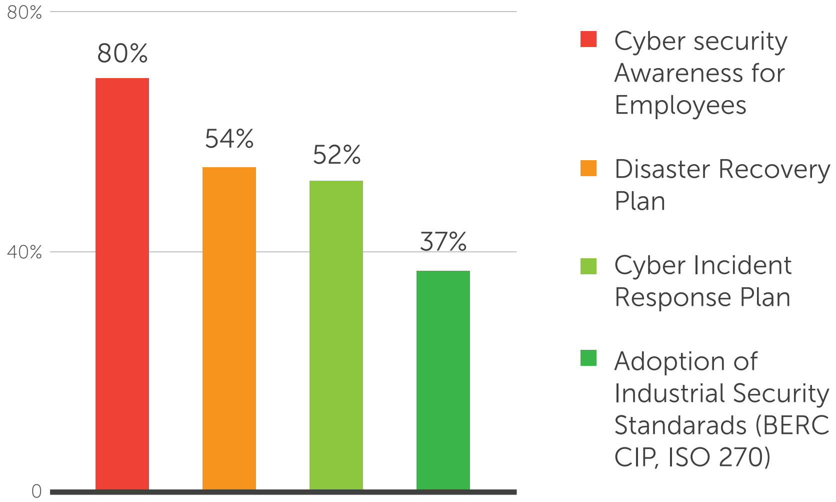
What sort of technical cybersecurity measures does your organization have in place to protect critical information systems?



Cybersecurity Policies

- Almost 70% of those surveyed have Cybersecurity Awareness Programs for employees. More than half have a Disaster Recovery Plan and/or Cyber Incident Response Plan in place.

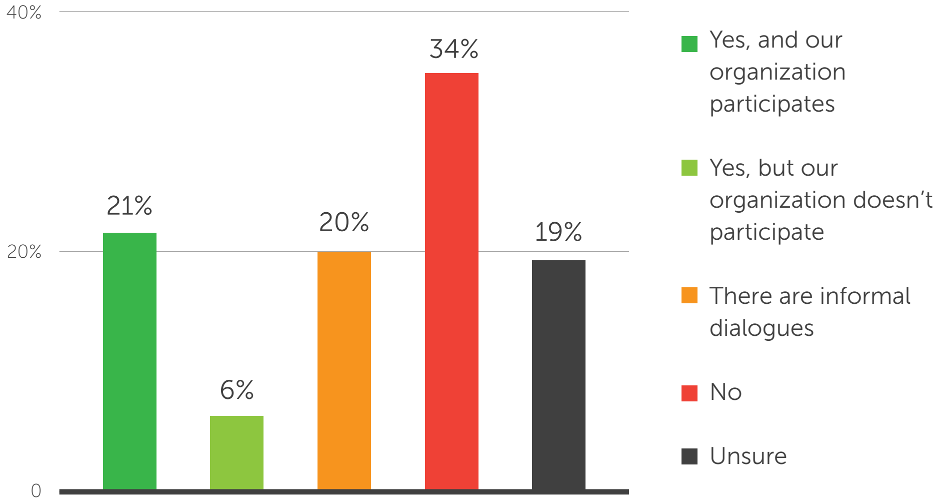
Does your organization have cybersecurity policies and/or plans?



Discussion with Government about Cyber Resilience of Critical Infrastructure Systems

- Almost half of the organizations reported there are discussions or informal dialogues with government about the cyber resilience of critical infrastructure systems.

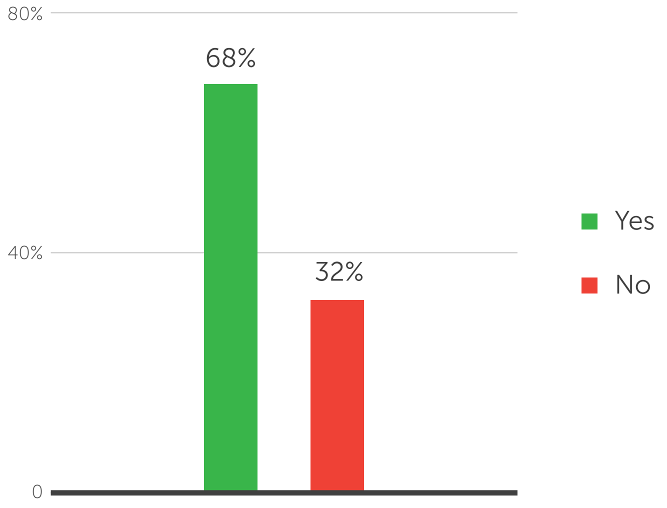
Is there a discussion/dialogue with government about the cyber resilience of critical infrastructure systems?



If Respondents trust the Government to advance a Cybersecurity Agenda in Critical Infrastructure Industries

Overall the majority of the organizations surveyed trust the government to advance a cybersecurity agenda in critical infrastructure industries, and are willing to work with the government.

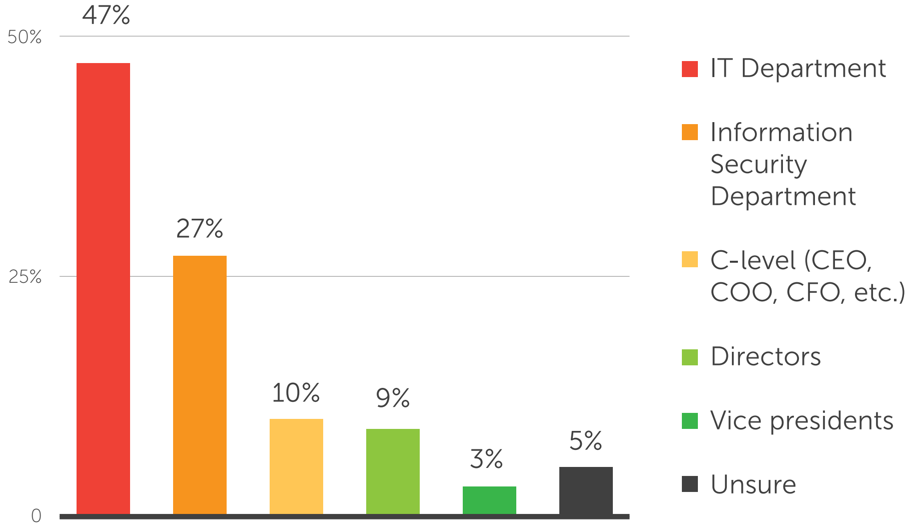
Do you trust the government to advance a cybersecurity agenda in critical infrastructure industries? How willing are you to work with them?



Level of Management that Supervises Cybersecurity

- Overall, the IT department is most likely to supervise organizational cybersecurity, particularly in Brazil.

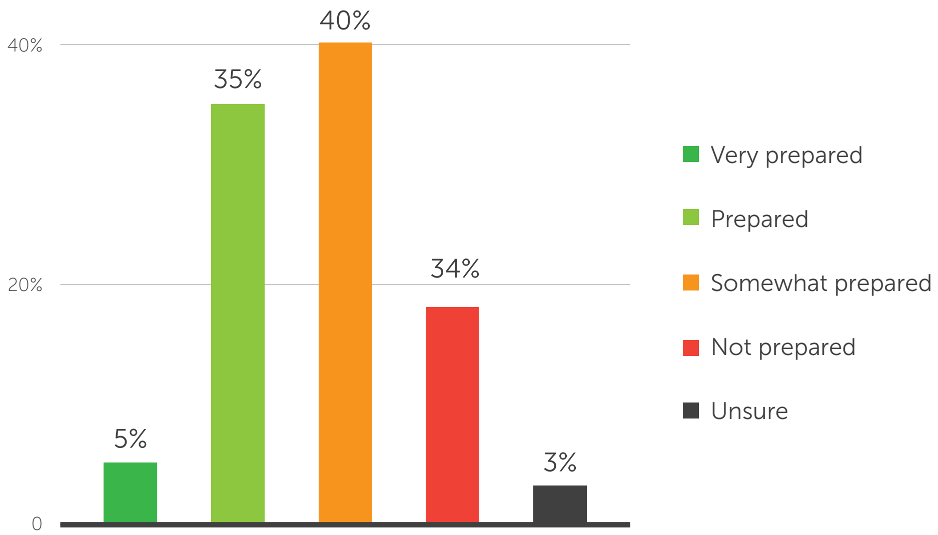
What level of management supervises organizational cybersecurity



Preparedness for Cyber Attack

- Almost half of the organizations reported there are discussions or informal dialogues with government about the cyber resilience of critical infrastructure systems.

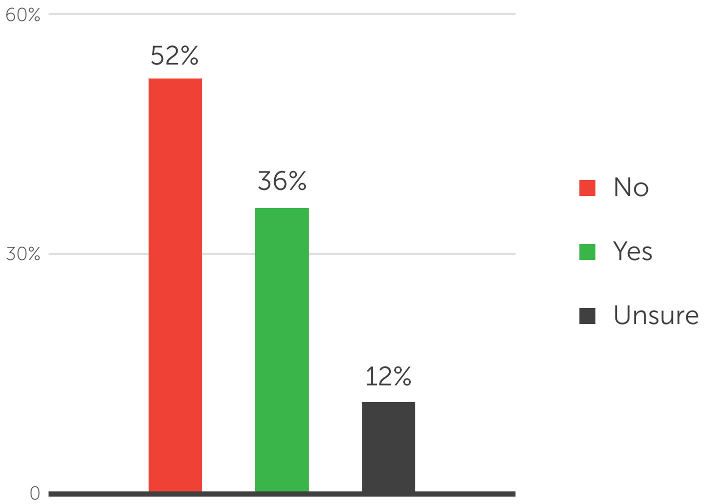
How prepared do you feel your organization is for a cyber incident?



Budget for Cybersecurity

- Overall the majority of the respondents reported their budget for cybersecurity did not increase over the last year.

Has your budget for cybersecurity increased over the last year?



Disclaimer

The contents of this publication do policies of the OAS do not necessarily reflect the views or policies of the OAS or contributory organizations.

Aviso importante

Los contenidos de esta publicación no reflejan recesariamente los puntos de vista de la OEA o de alguna de las organizaciones contribuyentes.

April 2015 / Abril de 2015

1889 F Street, N.W., Washington, D.C., 20006
United States of America

www.oas.org/cyber/

Organization of American States

Secretary General
José Miguel Insulza

Assistant Secretary General
Albert R. Ramdin

Secretary for Multidimensional Security
Adam Blackwell

Report on Cybersecurity and Critical Infrastructure in the Americas

Reporte sobre seguridad cibernética e infraestructura crítica en las Américas

Executive Secretary of the Inter-American Committee against Terrorism
Neil Klopfenstein

Editors
Tom Kellermann
Pablo Martinez
Belisario Contreras
Barbara Marchiori

Contributors
Kerry-Ann Barrett
Diego Subero
Gonzalo García-Belenguer
Emmanuelle Pelletier
Francisco Javier Villa
Geraldine Vivanco
Kyle Wilhoit
Christopher Budd
Ina Li
Paul Oliveria
Danielle Veluz

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569,8900