COMPENDIUM

Protecting strategic sectors from cyberattacks: Multistakeholder perspectives

December 2023

Microsoft

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

About this compendium

The compendium titled *"Protecting strategic sectors from cyberattacks: Multistakeholder perspectives"*, jointly authored by the Brazilian Center for International Relations (CEBRI) and Microsoft, is a pioneering collaboration in the pursuit of enhancing cybersecurity within the healthcare, finance, and energy sectors. Drawing on the collective knowledge of the broader multistakeholder community of experts who shared their insights throughout a series of workshops, the compendium provides an in-depth analysis of good practices and recommendations on cybersecurity hygiene. It not only underscores the critical importance of safeguarding these key sectors against cybersecurity threats, but also offers actionable and operational take-aways for stakeholders in both the public and private sectors. This comprehensive resource is a testament to the commitment of CEBRI and Microsoft to fostering a secure digital landscape across critical industries in Brazil and beyond.

The insights and ideas captured in these discussions and reported in this compendium reflect the diverse perspectives and expertise of a broad multistakeholder group, not necessarily the views of any one individual participant or the organizers of this project.

Contents

Foreword

Constant technological progress and the adoption of digital tools across sectors introduce new opportunities, but also create new risks for individuals, organizations, and governments. The increased use of internet-facing devices of all kinds, as a component of accelerating digital transformation, has greatly expanded the digital attack surface. This has resulted in an increase of nation state offensive cyber activity, as well as attacks conducted by criminal networks. Ransomware, for example, has become a sophisticated industry with groups dedicated to specific tasks performed as part of extortion. Attacks against strategic sectors, such as health, finance and energy, can generate large-scale consequences that can threaten human life, halt financial services, and disrupt power grids.

Fortunately, there are measures that can be taken to mitigate these threats. According to the 2023 Microsoft Digital Defense Report,[1] basic cybersecurity hygiene practices,[2] such as implementing multifactor authentication (MFA), applying Zero Trust principles,[3] using modern anti-malware, keeping software up-to-date, and protecting data can prevent 99 percent of attacks. However, despite a decade of calls for action and available guidelines, implementation is still lacking.

To help address this issue, the Brazilian Center for International Relations (CEBRI) and Microsoft organized a set of four workshops that explored the risks posed by cyberattacks against strategic sectors in Brazil, Latin America, and globally. The first workshop focused on prevalent cybersecurity threats and how cybersecurity hygiene practices could be a key part of addressing them and mitigating risks. The next two workshops focused on sectors that are at different stages in their cybersecurity hygiene maturity: the healthcare sector as relatively less mature and the finance and energy sectors as comparatively more established sectors with key learnings.[4] Finally, the last workshop reflected on the series as a whole and sought to bring forward lessons that applied across the topics discussed.

In sum, this workshop series aimed to identify lessons learned and recommendations to avoid and/ or mitigate the effects of cyberattacks on strategic sectors. It brought together members of the multistakeholder community across public, private, and non-profit entities and culminated in the development of this compendium on good cybersecurity hygiene practices. It also includes regional expert contributions from civil society, government, industry, and academia who provided insights on some of the main cybersecurity threats faced by strategic sectors and ways to address risks.

We believe that the recommendations contained in this *"Protecting strategic sectors from cyberattacks: Multistakeholder perspectives"* compendium can inform discussions on cybersecurity hygiene taking place both domestically and internationally. We also wish to thank all of our expert contributors for taking the time to provide their perspective on ways to mitigate risks, particularly in a Latin American context, and to all speakers who actively engaged in this project.

Microsoft

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

1 Microsoft Digital Defense Report, 2023
2 Cybersecurity hygiene is defined as a set of practices organizations and individuals can perform regularly to maintain the health and security of users, devices, networks, and data.
3 Zero Trust is a cybersecurity strategy that eliminates implicit trust and continuously validates every stage of a digital interaction. It is based on the principle of "don't trust anyone" and requires that anyone and everything trying to connect to an organization's systems must first be verified before access is granted. More can be learned from this Microsoft Security blog, 2023
4 Cybersecurity Optimization Platform (CYE), Cybersecurity Maturity Report, 2023

Introduction

Cybersecurity is a defining challenge of our time. Organizations of every size across every industry around the globe feel the urgency and pressure of protecting and defending against increasingly sophisticated attacks. Well-resourced cybercriminal syndicates continue to evolve and have developed into a cybercrime-as-a-service ecosystem that launches attacks at scale. Ransomware remains a key threat here. According to the 2023 Microsoft Digital Defense Report,[5] human-operated ransomware attacks are up more than 200 percent in the past year. There has also been increasing offensive activity from government actors. After last year's flurry of high-profile cyberattacks, state actors this year directed the bulk of their activity toward cyber espionage. Strategic sectors, the focus of this compendium, remain a key target with threat actors employing stealthier techniques to establish persistence and evade detection. This is all coupled with the unchecked expansion of the cyber mercenary[6] marketplace, which threatens to destabilize the broader online environment.

With that background, it was of paramount importance to examine the healthcare, finance, and energy sectors in the context of cybersecurity. These sectors are critical components of a nation's infrastructure. Disruptions in healthcare can directly impact patient care and safety, while financial institutions are responsible for safeguarding individuals' assets and maintaining economic stability. The energy sector plays a fundamental role in powering a nation's infrastructure and, therefore, its resilience is of strategic importance. The interconnectedness of these sectors amplifies their significance. As such, cyberattacks on one sector can have cascading effects, affecting the reliability and security of others. For instance, an energy sector breach can disrupt healthcare facilities' operations or lead to financial fraud. Therefore, understanding and fortifying the cybersecurity of these strategic sectors is imperative to ensure the overall resilience and stability of a nation's infrastructure and the well-being of its citizens.

Informed by the workshops that took place for this compendium five key recommendations surfaced:

A. Promote cybersecurity hygiene practices across all sectors.

Encourage all relevant stakeholders, including individuals, businesses, and government agencies, to prioritize and adopt fundamental cybersecurity hygiene practices. Cybersecurity hygiene should be ingrained as a routine, just like personal hygiene, to reduce the risks associated with cyber threats. These recommended practices include the implementation of MFA, Zero Trust principles, modern anti-malware solutions, regular system updates, and data encryption. By adhering to these practices, stakeholders can significantly enhance their cybersecurity posture.

B. Remain vigilant and go beyond minimal cybersecurity standards.

Online threats evolve constantly, necessitating a continuous journey of enhancing protocols and practices. Staying ahead of attackers means understanding the latest threats, adopting innovative technologies, and keeping pace with evolving cyber defense strategies. Leveraging new technologies, in particular artificial intelligence (AI) to enhance cyber threat detection and to identify cybersecurity trends, was raised in this context. Furthermore, organizations should invest in their employees by offering comprehensive cybersecurity training programs, transitioning away from compliance-focused annual trainings in favor of practical, hands-on learning opportunities.

5 Microsoft Digital Defense Report, 2023

6 Companies - or occasionally individuals - dedicated to developing, selling, and supporting offensive cyber capabilities which enable their clients - often governments - to access networks, computers, phones and internet-connected devices.

C. Build global cyber resilience.

The interconnected nature of the internet means that poor cybersecurity practices in one region can inadvertently affect others worldwide. Stakeholders should work together to develop and implement mechanisms for capacity building, leveraging international forums for collaboration. Additionally, building capacities to educate users about the risks associated with divulging sensitive biometric data is essential, especially as organizations increasingly use biometrics for security purposes.

D. Leverage international standards and collaboration.

Governments should engage in international collaboration and draw from existing global best practices when developing and implementing cybersecurity measures. This includes learning from the experiences and successes of other countries and leveraging established standards, laws, and regulations. Promoting effective responses to cybersecurity threats and ensuring alignment in approaches is particularly critical in the context of the global internet. Seeking opportunities to harmonize cybersecurity measures and standards will ultimately enhance global resilience to cyber threats. Collaboration within international organizations, such as the United Nations, can help facilitate this process.

E. Collectively work across the multistakeholder community to create a cybersecurity culture.

Creating a cybersecurity culture requires active engagement of civil society, academic institutions, governmental bodies, and industry stakeholders. The primary objective should be the dissemination of fundamental cybersecurity education across diverse age groups, with a strong emphasis on imparting practical skills and knowledge that everyday citizens require for their routine technology usage. By fostering a culture of cybersecurity awareness and preparedness, the multistakeholder community can empower individuals to navigate the digital landscape securely, thereby contributing to enhanced online safety and resilience for society as a whole.

Promoting cybersecurity hygiene practices, continuous vigilance beyond minimal standards, capacity building, leveraging international standards and collaboration, and embracing a multistakeholder approach stand out as paramount strategies to enhance cyber resilience across the health, finance, and energy sectors. Governments, industry, and civil society must collaborate, innovate, and invest in cybersecurity practices and technologies to mitigate evolving threats effectively. As such, these recommendations provide a blueprint for a holistic approach to address the complex cybersecurity challenges of our time, emphasizing the shared responsibility of all stakeholders to secure the digital realm and protect against cyber threats.

THEMATIC WORKSHOP 1:

Cyber threats and hygiene

The first thematic workshop positioned the concept of cybersecurity hygiene as the foundation of effective cybersecurity and societal resiliency. It was noted that notorious ransomware incidents have crippled entire federal entities and local governments, e.g., Brazil's judicial courts[7] and the Costa Rican government.[8] Tellingly, many of the security issues and vulnerabilities associated with those attacks derived not necessarily from the sophistication of the threat actors, but from a lack of implementation of cybersecurity hygiene practices and protocols. This premise complements Microsoft's finding referenced above, that the vast majority of successful cyberattacks, potentially up to 99 percent of them, could be prevented by implementing basic cybersecurity hygiene practices[9]. Relatedly, a recent study based on real-world attack data found that MFA reduces the risk of compromise by 99.2 percent.[10]

Building on the question of basic practices, another pivotal topic that was discussed at length was cybersecurity education, which was deemed critical to foster a culture of cyber resilience. This would need to take into account different factors, including access to education on this subject, demographics, and literacy rates.

The role of regulation was also touched upon. Countries have typically been quite reactive when it comes to cybersecurity threats, choosing to act in response to a large incident. Acknowledgement of this point was followed by calls for regulatory harmonization within and across borders and an emphasis on the need for governments to leverage existing frameworks. The Network and Information Security (NIS) 2 Directive, a foundational European Union (EU) law on cybersecurity, was discussed in this context.[11]

Finally, the workshop reinforced the key and necessary role the multistakeholder community plays. Forums that bring together relevant stakeholder groups and allow for the sharing of experience, expertise, and lessons learned help de-mystify the topic and lead to better outcomes that increase cybersecurity overall. Moreover, an assumption was made that working together to generate practical and interoperable measures aligned with international standards will likely lead to more global advancements on this issue.

7 The Bleeping Computer, Brazil's court system under massive RansomExx ransomware attack, 2020
8 The Guardian, Costa Rica declares national emergency amid ransomware attacks, 2022
9 Microsoft Digital Defense Report, 2023
10 ArXiv, How effective is multifactor authentication at deterring cyberattacks?, May 2023
11 European Parliament, The Network and Information Security (NIS) 2 Directive: A high common level of cybersecurity in the EU, 2023

Actionable recommendations informed by good practices and lessons learned included:

- **All stakeholders should adopt basic cybersecurity hygiene practices to decrease risk.** Good cybersecurity hygiene is the foundation of effective cybersecurity. As such, it needs to be treated just like personal hygiene and become a habit all users develop and implement. Recommended practices include 1) enabling multi-factor authentication, 2) applying Zero Trust principles, 3) using modern anti-malware, 4) keeping systems up-to-date, and 5) protecting data through encryption.
- **All stakeholders should assess the human rights implications of the cybersecurity measures they implement.** Taking human rights into account becomes essential when identifying and operationalizing good cybersecurity hygiene practices. The need to improve cybersecurity can never work against basic human and individual rights, infringing on a user's privacy or compromising their personal freedoms. Both need to be pursued together to effectively promote freedom and security.
- **Governments should promote more science, technology, engineering, and mathematics (STEM) education across communities.** To address challenges related with a lack of skilled cybersecurity professionals, governments should encourage greater access to STEM education, as well as incentivize prospective students to attend those courses. To grow the talent pipeline overtime, STEM curricula should be integrated in schools and universities much more comprehensively.
- **Governments should leverage international standards and seek harmonization when developing measures to tackle cybersecurity threats.** Rather than reinventing the wheel, governments should explore, learn from, and build on good practices, laws, standards, and regulations that have been effective in other countries. This will allow them to leverage the lessons learned by others, act quickly, as well as align approaches, which is critical with a global internet.
- **Governments should develop and implement plans to regularly and meaningfully engage the multistakeholder community on cybersecurity hygiene.** By creating a forum focused on a specific aspect of cybersecurity hygiene that brings together experts across the multistakeholder community, governments would help improve broad awareness of the threats societies face online.
- **Cybersecurity professionals should utilize the latest technologies and innovations to stay ahead of threats.** AI is one of the most promising technologies that can enhance cybersecurity and provide a competitive edge. It can give the defender an asymmetric advantage by helping automate and augment many aspects of cybersecurity, such as threat detection, response, analysis, and prediction.
- **Governments should leverage international forums to collaborate with stakeholders from industry and civil society to organize joint assessments of cyber challenges.** Multistakeholder assessments would create buy-in and help identify practices that are interoperable with existing international standards.

Recommended readings and resources shared by participants:

- Agência Nacional de Telecomunicações/ National Telecommunications Agency (ANATEL), Overview of cybersecurity regulations, 2023
- Charter of Trust, Secure Development Lifecycle: Step-by-step Guidelines, 2022
- Brasscom, ICT Talent Demand and Strategy Σ TCEM, 2021
- European Parliament, The NIS2 Directive: A high common level of cybersecurity in the EU, 2023
- Microsoft Digital Defense Report, 2022
- Microsoft Digital Defense Report, 2023

Contributions by experts:

What are some of the main cybersecurity threats faced by strategic sectors, and what are your recommendations to prevent them or mitigate their effects?

Cybersecurity and digital transformation are at the core of achieving sustainable development in Latin America. However, with government departments often driving digital and cybersecurity agendas in distinct silos, coordination, which is key for elaborating and implementing an effective and durable strategy, can be stifled. Such synergies are also only possible if governments have a calibrated perspective of where to start implementing cybersecurity measures. Efforts to generate better cyber resiliency are not necessarily aided by focusing on remediating large-scale incidents. While it might seem that the region is perhaps more susceptible to ransomware than other locations - given the cases in Costa Rica,[12] Colombia,[13] and Brazil[14]- a ransomware attack is inevitably only as effective as its 'seed', which is sometimes a mere phishing email. While sophisticated attacks drive headlines, developing countries – especially in Latin America – cannot afford to leave cybersecurity hygiene unaddressed, particularly across strategic sectors, and need to make it both a political priority and a multistakeholder effort.

However, sustainable digital development counts little if trust in technology is undermined by the misuse of cyber capabilities from governments in the region. Both the private sector and governments have a shared responsibility to respond to the disproportionate human rights and privacy-related impacts of the use of technologies, such as commercial hacking tools. We need to ensure the responsible and accountable use of technologies in tandem with upskilling the population.

While most of the media coverage on commercial hacking tools focuses on highly intrusive spyware such as Pegasus,[15] it is in the grey zone between bespoke technologies and open-source intelligence tools where the challenge lies. It is imperative to determine the necessary checks and balances on these tools' acquisition and use, particularly as developing countries increasingly look at outsourcing to enhance their capabilities to tackle domestic threats. Earlier in 2023, countries such as Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the UK, and the US issued a joint declaration calling for international controls on the proliferation of commercial spyware.[16] Similarly, private sector entities involved in the Cybersecurity Tech Accord proposed a set of principles to counter the proliferation of cyber mercenaries and commercial hacking tools.[17]

Despite these efforts, there is still a long way to go before we can expect to see developing countries reflect, respond, and engage in this debate. Latin America, for example, has reportedly and historically been interested in the use of such tools, with countries such as Brazil and others having attempted to acquire such capabilities.[18] Rather worrying about not being able to access these types of technologies, democracies should seek to actively promote a rights-respecting cyberspace while engaging in an evidence-based dialogue on capacities and the use of technologies with accountability and controls put in place. This feeds into the need to implement cybersecurity hygiene good practices and advance societal resiliency, ultimately defending against threats that could target strategic sectors that we all rely on.

***Louise Marie Hurel S. Dias**, PhD Candidate of Data, Networks, and Society at the London School of Economics and Political Science*

12 The Guardian, Costa Rica declares national emergency amid ransomware attacks, 2022
13 Reuters, More than 50 Colombian state, private entities hit by cyberattack -Petro, 2023
14 ZDNET, Brazilian government recovers from "worst-ever" cyberattack, 2020
15 The Citizen Lab, Pegasus vs. Predator, 2021
16 The White House, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, 2023
17 Cybersecurity Tech Accord, Cyber mercenaries: An old business model, a modern threat, March 2023
18 Business & Human Rights Resource Centre, Brazil: Million-dollar negotiation for the Pegasus espionage programme, 2021

THEMATIC WORKSHOP 2:

Strategic sectors with relatively low cybersecurity hygiene maturity (health sector)

Modern hospitals are digitally connected and increasingly rely on technology to provide care. During the second thematic workshop, participants agreed that one of the most worrying trends of recent years has been an exponential growth in cyberattacks on healthcare organizations. This sector is increasingly targeted, including through ransomware attacks, with potentially significant harm to patients. These attacks can breach confidential data, disrupt care and emergency services, and allow access to essential services. This means that people working in the healthcare sector, such as doctors and nurses, need to receive training on good cybersecurity hygiene practices.

The session included cybersecurity practitioners identifying several key structural changes that need to take place to increase the healthcare sector's cybersecurity hygiene maturity. The importance of changes in the management culture of healthcare facilities was cited multiple times. In today's societies, the processes designed to increase cybersecurity are often perceived as obstructions imposed at the management level, slowing down medical care delivery to patients. As a result, cybersecurity hygiene is often seen as additional costs competing with the provision of care, rather than as an enabler of care. A positive shift in institutional culture is needed to ensure that all stakeholders, including the leadership within healthcare organizations, take cybersecurity into careful consideration and implement cybersecurity hygiene practices tailored to this sector.

Actionable recommendations informed by good practices and lessons learned:

- **Healthcare organizations should develop an action plan to overcome the divide between healthcare practitioners and IT teams.** While IT teams tend to emphasize cybersecurity, healthcare practitioners and the management of healthcare institutions tend to focus on patients' health. Such a strict divide is no longer tenable. On the contrary, investments in both medical care and cybersecurity need to be seen as mutually reinforcing, rather than as tradeoffs. The procurement of medical services that rely on technology needs to have cybersecurity at its heart, rather than be seen as an additional strain on stretched resources.
- **Healthcare entities should develop risk management strategies for prevention, detection, and response to cybersecurity threats and ensure that these strategies are embraced at all organizational levels.** Participants highlighted that the healthcare sector tends to be quite hierarchical, with the top management consisting predominantly of medical professionals who tend to underestimate cybersecurity risks. An open culture needs to be encouraged and cultivated so that all staff, including IT professionals, feel empowered to speak up and communicate their cybersecurity concerns to management.
- **Guidelines and cybersecurity hygiene measures for personal devices of medical staff and connected medical devices should be put in place.** This is key as the number of such devices used in healthcare facilities has increased dramatically in recent years. Personal and connected devices are usually insufficiently secured and add a new vector of

compromise to the sector. Multi-factor authentication should be implemented across the sector.

- **Healthcare entities should proactively reach out to and partner with the technology sector to continuously improve their systems.** This could include developing and implementing systems, including leveraging AI that proactively monitors the threat landscape, learns from patterns, and detects and provides early warnings about potential threats.
- **Manufacturers should ensure frequent patching cycles of medical devices.** Currently, patches can be rare or even non-existent, which means medical devices do not benefit from new cybersecurity protective measures, leaving these devices vulnerable to attacks. Available patches should be regularly and systematically implemented in medical facilities. The importance of firewalls was also emphasized.
- **Healthcare entities should develop action plans and regularly assess the complexity of data systems that require protection.** Currently, data is often widely dispersed and not integrated, which makes protection much more challenging. Migrating data to the cloud was recommended as a reliable way to scale up cyber defenses.
- **Healthcare entities should incorporate resilience and backup measures into their crisis planning.** This would allow for their overall systems to keep working even when parts of it fail. As such, it should ensure access to critical data even if a network or parts thereof go down due to a cybersecurity incident. Continuously testing their readiness by engaging in cybersecurity exercises is recommended.
- **Stakeholder groups across government, industry, and civil society should focus on capacity building as an essential part of improving the cyber resilience of the healthcare sector.** However, capacity building is a resource-intensive undertaking, which may be hard to prioritize in an often under-resourced and overburdened healthcare sector. To overcome these challenges, the broader multistakeholder community can help healthcare entities learn from other fields with more experience in implementing cybersecurity hygiene practices.
- **Capacity building should be discussed in regional and global forums.** These forums can include the World Health Organization (WHO), the UN more broadly, and the Global Forum for Cybersecurity Expertise (GFCE). Discussions at this level can help facilitate information sharing and drive capacity building across the globe.
- **Governments should amplify real-life, human costs of cyberattacks.** The human costs of cyberattacks against strategic sectors and messaging calibrated to generate political will to increase investment into healthcare sector cyber resilience is key. Specifically, systematically mapping the global impact of cyberattacks against the healthcare sector was highlighted as a means to empower the wider multistakeholder community with evidence to make progress in their respective work and advocacy.
- **Healthcare entities should embrace a multistakeholder approach to identify hygiene practices that best address existing gaps.** Similar to the findings from the first thematic workshop, all relevant actors need to be included in addressing cybersecurity, such as relevant state officials, first responders, private sector representatives, and civil society organizations in the discussion. This would help surface the latest information on cybersecurity threats facing the sector to fill existing gaps with good practices.

Recommended readings and resources shared by participants:

- CyberPeace Institute, Cyber Incident Tracer #HEALTH (CIT),2022
- CyberPeace Institute, Microsoft, Ministry of Foreign Affairs of the Czech Republic, National Cyber and Information Security Agency of the Czech Republic (NÚKIB); Compendium of Multistakeholder Perspectives; 2022
- European Union Agency for Cybersecurity (ENISA), Procurement Guidelines for Cybersecurity in Hospitals, 2020
- European Union Agency for Cybersecurity (ENISA), Cloud Security for Healthcare Services, 2021
- European Union Agency for Cybersecurity (ENISA), Good practices for the security of healthcare services (ENISA), 2023
- Global Forum on Cyber Expertise (GFCE), Strengthening cyber capacity and expertise globally through international collaboration,2023

Contributions by experts:

What are some of the main cybersecurity threats faced by the healthcare sector, and what are your recommendations to prevent or mitigate them?

The healthcare sector faces numerous cybersecurity threats, which can have severe consequences for patient safety, data privacy, and the overall functioning of healthcare organizations. Here is a list of some of the main threats and recommendations to avoid or mitigate their effects:

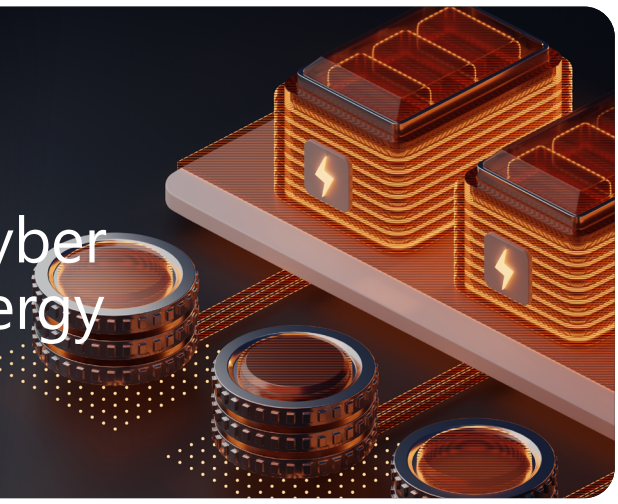
- **Ransomware Attacks:** Ransomware attacks can encrypt patient data and demand a ransom for decryption keys, disrupting healthcare operations. Some recommendations to address this threat include: regularly backing up data and systems off-line; educating staff about phishing and suspicious e-mails; keeping software, cloud, and security systems up to date; and developing an incident response plan.
- **Data Breaches:** Unauthorized access or theft of patient records can lead to identity theft, fraud, and privacy violations. Some recommendations to address this threat include: encrypting sensitive patient data; implementing strong access controls and authentication mechanisms; and conducting regular security audits and vulnerability assessments.
- **Insider Threats:** Employees or insiders with access to systems can intentionally or unintentionally compromise data security. Some recommendations to address this threat include: monitoring user activity and implementing user behavior analytics; conducting security awareness training for staff; and limiting access to sensitive information based on job roles.
- **Phishing Attacks:** Phishing emails can trick healthcare staff into revealing login credentials or downloading malicious attachments. Some recommendations to address this threat include: training employees to recognize phishing attempts; implementing email filtering and authentication mechanisms; and using MFA for access.
- **Third-Party Risks:** Vendors and partners may have weaker security measures, providing attackers with a pathway into the healthcare network. Some recommendations to address this threat include: establishing strong security agreements with vendors and monitoring vendor access and activities.

Regarding incident response planning, it is recommended to develop a comprehensive incident response plan, conduct tabletop exercises to test the plan's effectiveness, and continuously improve incident response based on lessons learned. It's essential to foster a culture of cybersecurity awareness and responsibility within healthcare organizations. Regular training and awareness programs can help staff understand the importance of their role in safeguarding patient data and the overall security of the organization.

Ministry of Health of Brazil

THEMATIC WORKSHOP 3:

Strategic sectors with comparatively high cyber hygiene maturity (energy and financial sectors)



In today's interconnected world, where digital technologies drive innovation and productivity, robust cybersecurity measures are paramount for organizations operating in strategic sectors. This third workshop delved into the crucial topic of cybersecurity hygiene within the finance and energy sectors. These industries have become prime targets for online threats. Financial institutions, which handle large volumes of sensitive customer information and financial transactions, are particularly attractive targets for cybercriminals. Similarly, the energy sector faces threats ranging from disruptive attacks on power grids to espionage targeting valuable intellectual property.

Per the Microsoft's 2023 Digital Defense Report, cyberattacks can be operated as a service and phishing, identity, and distributed denial of service (DDoS) attacks can now be launched at scale.[19] As a consequence, there is a growing number of online services facilitating various cybercrimes, including Business Email Compromise (BEC) and human-operated ransomware. Phishing continues to be a preferred attack method as cybercriminals profit significantly from successfully stealing and selling access to stolen accounts. Moreover, critical infrastructure remains a popular target, with threat actors employing stealthier techniques to establish persistence and evade detection.

In light of these developments, the participants in the third workshop reinforced the need to maintain robust cybersecurity practices to protect both sensitive data and strategic sectors in order to ensure uninterrupted operations. They highlighted lessons from the finance and energy sectors that could be applied to other strategic sectors with comparatively less mature cybersecurity practices. Recommendations regarding establishing trusted networks across stakeholder groups before incidents occur and issuing regular guidelines and updates for coherent sector good practices were also emphasized throughout.

Actionable recommendations informed by good practices and lessons learned:

- **Governments should issue cybersecurity guidelines and regularly update them.** A concrete example is Brazil's National Electric Energy Agency (Agência Nacional de Energia Elétrica, ANEEL),[20] which regulates the electric power market in Brazil. ANEEL has established a multidisciplinary and cross-sector committee that covers strategic sectors and reviews incidents once a month. It issues cybersecurity guidelines, including indicators of compromise, releases ongoing cyber-related assessments, and shares updates on incidents and good practices.

19 Microsoft Digital Defense Report, P. 13, 2023
20 Agência Nacional de Energia Elétrica/ National Electric Energy Agency (ANEEL)

- **Operators across strategic sectors and governments should maintain a continuous inventory of all OT devices.** In looking at the security challenges that arise from the convergence of information technology (IT) and operational technology (OT) for government departments, it is also necessary to maintain a real-time, continuous inventory of all OT devices, software, systems and assets.
- **Operators across strategic sectors should leverage new technologies to enhance threat detection and identify cybersecurity trends.** New technologies, such as AI, can help by automating and augmenting many aspects of cybersecurity, such as threat detection, response, analysis, and prediction. For example, Brazil's energy sector has started to leverage AI to identify trends and to standardize cybersecurity measures aimed at generating more resiliency throughout.
- **Operators across strategic sectors should assess the advantages and disadvantages of having centralized technology systems versus decentralized systems.** There are both benefits and risks associated with having systems either centralized or decentralized. On the one hand, a centralized system is easier to control, monitor, and ultimately more efficient to coordinate. However, it can concentrate systemic risks. As such, it is important to implement a secure architecture, continuously evaluate threats and risks, and make necessary adjustments to prioritize cybersecurity.
- **Strategic sectors should establish trusted communities for effective information sharing.** Effective information sharing should contain at least the following elements: a) focus on voluntary sharing, b) identify opportunities for cross-sectoral sharing, c) build trust among the actors involved, and d) ensure there is clarity on who reports to whom and what happens with the data. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a particularly good framework for information sharing that could serve as a model for comparatively less mature sectors.
- **Governments should work with the multistakeholder community to proactively deter cybercrime.** One way to tackle cybercrime is to quickly and meaningfully disrupt the technical infrastructure (e.g., virtual machines, emails, homoglyph domain names, public block-chain web sites, etc.) used by cybercriminals, forcing them to lose their investments as quickly as they make them. Governments, working with the multistakeholder community, should take coordinated technical and legal action to prevent cybercriminals from effectively abusing technology.
- **Operators across the finance and energy sectors should create a cybersecurity conscious culture by providing cybersecurity-related materials all customers can understand.** Every day citizens rely on the essential services provided by both the finance and energy sectors. This calls for the need to generate a cybersecurity conscious culture. This may come in the form of providing resources to integrate cyber education from kindergarten all the way through grade school, sponsoring scholarships for students in need, and continuously raising awareness about systemic risks. Working with local community groups that can both distill information and reach different audiences is another way to reach comparatively vulnerable target audiences.
- **Cybersecurity professionals should spur voluntary information sharing by building interpersonal relationships.** Interpersonal relationships and trust between cybersecurity professionals across strategic sectors is crucial. Trusted relationships create an atmosphere with certain mutual expectations about behavior. Reciprocity can be a strong factor in driving cooperation in collective action problem scenarios. If members of an information exchange program expect that their counterparts, even those in direct competitive relationships, are acting in good faith, they are more likely to share information on threats and vulnerabilities.
- **Cybersecurity professionals should make full use of information shared by conducting analyses on long-term trends.** A greater understanding of the root causes of cybersecurity incidents can help prevent future incidents. In many cases, a detailed analysis of the incidents can inform the selection and prioritization of cybersecurity risk mitigations for organizations. The exchange of this information could improve critical infrastructure operations and help information and communication technology (ICT) vendors in the finance and energy sectors (and beyond) make products and services more resistant to abuse, compromise, or failures. Furthermore, such analyses can also help build knowledge of long-term trends, giving network defenders a better understanding of emerging cyber-threats and of shifts in exploitation methods.

Recommended readings and resources shared by participants:

- Microsoft's Digital Defense Report, 2023
- European Central Bank, Cyber Information and Intelligence Sharing Initiative (CIISI-EU), 2020
- Federal Financial Institutions Examination Council, Cybersecurity Resource Guide for Financial Institutions, 2022
- PricewaterhouseCoopers (PwC), Energy and utilities cyber outlook, 2022
- International Monetary Fund (IMF), The Global Cyber Threat, 2021
- Amy Hogan-Buney, Microsoft on the Issues, Stopping cybercriminals from abusing security tools, 2023

Contributions by experts:

What are some of the main cybersecurity threats faced by the energy sector, and what are your recommendations to prevent or mitigate them?

As process optimization in the energy sector increasingly relies on digitalization, this has resulted in an expanded focus on cybersecurity. Some of the more prominent threats include:

- **Supply chain attacks:** A cybersecurity compromise in a service or product managed by third parties with a lower level of cybersecurity maturity could seriously affect an organization's environment. What can be done? Organizations should assess and manage the cyber risks for third parties to ensure appropriate cyber resilience for their risk environment.
- **Ransomware attacks:** This is one of the most common and profitable attacks for cybercriminals, since organizations will pay to ensure their data is not released and returned to them. What can organizations do to defend against this? First, it is essential to properly train the users, since general infections by this type of malware always starts with a phishing attack. In this case, it is essential to have cyber-safe practices put in place prior to an incident. Other measures include having good incident management protocols to detect malware at an early stage, responding quickly to prevent it from spreading, and ensuring that there is a backup policy in place to restore and minimize the impact on business continuity.
- **Phishing and email fraud attacks:** Phishing campaigns are becoming more sophisticated and are now targeting specific users, making it more difficult for users to be alert and detect them in time. To address this, training and awareness are key, as well as good incident management insights.
- **Cyber espionage:** We have seen an increase in this type of cyberattack in the region in the last few years. Attackers seek to enter systems and stay hidden to steal as much information as possible. To defend against it, it is essential to protect the most sensitive information with solid policies and tools for handling confidential information.
- **Denial of service attacks (DoS) targeting critical infrastructure:** Although this type of attack is less common, determined hacktivists or malicious users can create severe disruptions by leveraging DoS. How can this be avoided? Having a deep-in-defense strategy supported by a comprehensive cybersecurity management program to protect our business and energy development is the only solution.

In a nutshell, to address these threats we must have a holistic and comprehensive cybersecurity program in place, adaptable to the changing and challenging environment, paired with strong stakeholder commitments.

***María Victoria Morrone**, Senior Cyber Security Officer at Siemens Energy Latin Americ*a

THEMATIC WORKSHOP 4:

Summarizing the series

The fourth and final workshop focused on the importance of augmenting cybersecurity hygiene across the strategic sectors, delved into some of the cross-sector differences and similarities, and provided an opportunity to talk about some of the main recommendations from previous events.

Kicking off with a question on how basic cybersecurity hygiene practices can effectively be promoted and implemented at both individual and organizational levels, participants stressed that cybersecurity is a continuous journey. Users need to understand why cybersecurity hygiene is relevant to them and the practical measures they can and should take to mitigate their own personal risks online. A recurring theme was the need to make recommendations relatable at an individual level. A suggestion on how to do that focused on showcasing the real-world consequences of cyberattacks on the lives of people.

Although there were clear differences identified between the three sectors discussed, the participating experts highlighted that most attacks are rooted in exploitation of basic entry points. Resolution 964 by the Brazilian National Electric Energy Agency was referenced as an example of rising awareness, as it requires organizations to notify the government of certain types of incidents. Participants explained that this requirement has gone some way to help overcome the desire to keep all incidents secret and encouraged a culture of information sharing within the country. Nevertheless, it was noted that when it comes to incident reporting the right balance needs to be achieved to ensure the focus remains on addressing the incidents and not reporting for reporting's sake.

Another theme that surfaced was the dramatic increase in remote work brought about during the COVID-19 pandemic. This made cybersecurity simultaneously more important and more complex for companies looking to safeguard their employees and data, even as many return to work from the office.

Actionable recommendations informed by good practices and lessons learned:

- **Governments should establish safe channels of communications to share information on cybersecurity threats.** Information sharing needs to be a two-way channel. When it comes to cybersecurity, the right information exchanged or shared at the right time can enable security professionals and decision makers to reduce risks, deflect attacks, mitigate exploits, and enhance resiliency. To establish a safe channel of communication, it is important to develop an overarching strategy for information sharing and collaboration, designed with privacy protections in mind, and establish a meaningful governance process that includes appropriate management of the data shared.

- **Organizations should remain vigilant, not merely meet minimum cybersecurity standards, but continuously seek to enhance protocols to stay ahead of advancing threats.** Cybersecurity is a continuous journey and organizations need to keep pace with the attackers by going beyond minimum standards and adopting security practices to be able to effectively defend themselves. It is therefore imperative that they understand the latest threats and follow and adopt the latest technological innovations and approaches.
- **Organizations should invest in their employees and continuously train them in the latest cybersecurity hygiene practices.** It is imperative that organizations transition from compliance focused cybersecurity trainings and adopt a multifaceted approach that supplements those efforts with practical, hands-on opportunities to learn the latest cybersecurity tools and techniques. This method fosters a deeper understanding of cybersecurity and the implications of legislative requirements.
- **All relevant stakeholder groups should focus on developing and implementing capacity building mechanisms.** In the past two decades, there has been some progress in establishing the international cybersecurity framework, through recognition of the application of international law to cyberspace and the adoption of the 11 UN norms on responsible state behavior in cyberspace, from 2015. Given the interconnected nature of the internet, poor cybersecurity hygiene in one country or region can impact others around the world. Investment in capacity building to ensure all countries can be cyber resilient is critical, and the multistakeholder community should leverage forums, such as the GFCE to that end.
- **Governments should create a worldwide directory for cybersecurity related points of contact (POCs).** Governments have a unique opportunity to implement a points of contact tool for reducing tension, minimizing the risk of misunderstandings, and building trust. Similar measures already exist at the regional level, for example at the Organization for Security and Co-operation in Europe (OSCE), however there is no such mechanism pulling together contacts across the diplomatic and technical communities available globally. Governments should advance discussions at the UN to establish such a database, in the context of the ongoing Open-Ended Working Group on cybersecurity.
- **All stakeholder groups should develop cybersecurity hygiene training programs to educate users about the potential risks associated with divulging sensitive information, such as biometric data.** Organizations are increasingly leveraging biometric data in research, but also for cybersecurity. However, unlike a hacked password, biometric data is immutable. If these databases were to be breached, it could pose a significant identity risk to users. To address these concerns, it is imperative that cybersecurity hygiene training programs educate users about the potential risks associated with divulging sensitive biometric data.

Recommended readings and resources shared by participants:

- Ministry of Mines and Energy/National Electric Energy Agency, ANEEL Normative Resolution Number 964, 2021
- United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015
- Organization for Security and Co-operation in Europe (OSCE), OSCE Guide on Non-military Confidence-Building Measures (CBMs)
- Cybersecurity and Infrastructure Security Agency (CISA), Cyber Hygiene Services, 2023
- Cybersecurity and Infrastructure Security Agency (CISA), Free Cybersecurity Services and Tools
- Microsoft, A framework for cybersecurity information sharing and risk reduction, 2015

Contributions by experts:

What are some pressing cybersecurity threats faced by strategic sectors, and what are your recommendations to prevent or mitigate their effects?

In the current global technological ecosystem, we can identify cybersecurity threats manifesting themselves in two primary ways: a) their direct utilization within the context of armed conflicts, essentially employed as instruments of warfare, and b) their exploitation in scenarios that promote social instability and facilitate online crimes. These two dimensions present substantial threats to both the state and society, demanding special attention from governmental authorities. These threats encompass activities such as industrial and state espionage; acts of sabotage; attacks involving unmanned aerial vehicles; theft of sensitive data from governmental entities, citizens, and private organizations; attacks on critical state infrastructure; and most notably, the manipulation of information technologies and communication channels to destabilize democratic institutions within states.

To confront this reality, a two-pronged approach is essential: one focused on prevention and the other on resilience. Prevention efforts should center on: a) formulating public policies and robust strategies that coordinate the state's cybersecurity capabilities to ensure swift and ongoing prevention of cyberattacks; b) establishing a dedicated state cybersecurity agency responsible for centralizing and coordinating both preventative measures and resilience strategies; c) promoting cybersecurity awareness among the general population, equipping them with the necessary technological knowledge to safeguard themselves and to effectively utilize emerging technologies and; d) pursuing the development of domestic technology expertise to reduce external dependence. To improve cyber resilience, it is advisable to: a) maintain an effective cybercrime combat unit operating at multiple levels, and b) develop and implement robust system recovery protocols for responding to cyberattacks, and ensuring that personnel are trained to react swiftly and can efficiently restore affected systems.

If we focus on Latin America and its geopolitical dimensions, we can conclude that the region represents one of the main hubs for the use of ICTs across two dimensions: a) the widespread use by the population, businesses, and states of digital resources to enhance everyday processes and b) the illegal use of these resources to commit cybercrime. The region must therefore consider the two dimensions noted above: prevention and resilience. However, a number of challenges still need to be overcome, including a) lack of state cooperation with the broader multistakeholder community in this field; b) lack of high-tech developments in the countries of the region, and c) lack of budget to invest in cybersecurity, cyber defense, and specialized personnel training in the field.

One of the paths to enhance cybersecurity policies and practices in the region is to make this issue central to the agenda of the region's governments. Effective public policies only emerge when their guiding theme becomes a priority on the political and budgetary agenda. Thus, in Latin America, cybersecurity needs to rise to the top of the agenda if we are to protect society, the private sector, and the state effectively and sustainably.

***Danielle Jacon Ayres Pinto**, Professor of International Relations at the Federal University of Santa Catarina*


Microsoft


CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS