Increasing Cybersecurity Capacity Through Connectivity and Digital Education

By: Andy Kotz and Camila Herrera

Latin America faces about 1,600 cyberattacks per second, 91% of Latin American companies have recorded a cybersecurity incident last year, and 62% have suffered a data breach. With data like this, it's no wonder The World Economic Forum's Global Risks Report 2024 ranked cybersecurity as the fourth most severe global risk in both the short and long term. In response to such a large-scale problem, policymakers often want to find ways to fix countries' cybersecurity infrastructure and incident response - both of which are problems in Latin America. However, to truly help the region develop technologically, we need to think more broadly about how to build a secure digital culture.

Connecting every single person to the internet sounds great, but when we forget about people as soon as they are connected, they become vulnerable due to the growing number of devices waiting to be compromised. To prevent this problem from spiraling, it's useful to think about the concept of 'flow security', the idea that security is not only tied to the protection of a particular entity or territory. Rather, security and connectivity grow *together*, supplementing each other. Reimagining this space by turning it into a collaborative environment in which governments, private sector companies, and individuals from all over the region work together to invest in connectivity is essential. With a collaborative model, and with digital literacy at the forefront, the region's cybersecurity capacities will grow exponentially.

Digital literacy and cybersecurity are closely intertwined concepts. The relationship between the two is evident: a strong understanding of the digital landscape enables individuals to identify suspicious situations and take measures to

protect themselves. As technology advances, hackers develop increasingly sophisticated methods, making critical thinking and information literacy indispensable skills for staying abreast of potential threats. Being able to discern reliable information from dubious sources is crucial in an era where misinformation abounds, ensuring that individuals aren't unwittingly deceived by infamous scams asking for money or passwords.

As USAID's Digital Ecosystem Framework highlights, "Digital technologies are becoming more accessible and have brought the promise of enormous benefits from digitalization." However, "they also present significant risks to privacy and security through surveillance, censorship, and other forms of digital repression." While increasing connectivity does come with inherent risks, the possibilities outweigh the potential risks. They can "advance freedom and transparency, generate shared prosperity, strengthen inclusions, and inspire innovation." Connectivity relates not just to policies, but "properties of how people can relate to each other." Connectivity refers to the connection between people, between cultures and ideas, as well as digital infrastructure. By building upon digital connectivity, the socio-cultural ties which bind us together can continue to strengthen. With a growing understanding of how security and connectivity work together, the region has the opportunity to build out its infrastructure in a way that fosters security.

Specifically, the region's digitalization encompasses more than just broadening Internet accessibility; it also entails the integration of new technologies into citizens' daily routines. This includes everything from mobile banking and online shopping to smart home systems. E-commerce is on the rise in the region, with experts projecting a 27% increase in transaction volume by 2023, reaching $509 billion. Approximately 66% of the adult population in Latin America shops online, with figures surpassing 80% in countries like Argentina, Brazil, Chile, and Colombia. Numerous countries, notably Brazil, Argentina, Mexico, Colombia, and Chile, have implemented national programs to foster the growth of the digital economy. These initiatives are designed to integrate emerging technologies across various sectors, particularly enhancing government services and advancing e-commerce and digital payment systems. Assessments such as the E-Government Development Index and the GovTech Maturity Index indicate that most countries in the region have achieved high or very high levels of digital development in their government services.

As governments transition to digital client portals and digital payment systems, it becomes essential for citizens to acquire the necessary skills to navigate these platforms securely. This includes identifying and safeguarding against

potential cyber threats, emphasizing the importance of digital literacy and cybersecurity education for all. Peru, for example, designed a National Digital Talent Strategy to "advance digital talent development, emphasizing diversity and an intercultural approach." By not only innovating in engineering and technology, but also the types of programs that follow, the country has increased its capacity to not only grow its economy, but to do so in a secure way.

As helpful as individual countries' programs are, security can't exist in silos. Cybercrime is often transnational, so when countries or companies isolate themselves, the cybersecurity threat only grows. Rather than isolating oneself as a means to protect, countries in the region should cooperate on ensuring the entire region creates a meaningful digital economy through connectivity and security. Just as *physical* connectivity increases trade, tourism, and cultural exchange, *digital* connectivity increases activity in the financial market, the flow of ideas, and much more.

How do we ensure connectivity fosters positive growth as opposed to simply increasing cybersecurity risks? The entire region must buy in. Ries believes that "asymmetry in dependence…plays to the benefit of the least dependent. Dependence in strategic sectors, for instance 5G technology, while environmentally or economically sound, can have adverse security implications." To ensure the region participates actively in cybersecurity, it needs not only an educated workforce, but also a community of digital citizens. **As connectivity grows, it is imperative for the region to prioritize investment in digital literacy. This will ensure that as connectivity expands, cyber threats do not escalate.**

Recommendations

Cooperation and innovation must spearhead the Latin American response to connectivity and cybersecurity issues. Innovation in the tech sector, but more importantly in the regulation of the sector, is critical. Creating national digital, cybersecurity, or digital workforce strategies will allow countries to tackle these issues from the root. It allows them to build a resilient digital workforce, which will allow them to be prepared for cyberattacks when they inevitably must react.

In a scenario where a government does not possess adequate resources to invest in digital literacy or technology, we recommend providing incentives to private companies for working in this space. Often, the knowledge and reach of companies is larger than that of the public sector, often due to budgetary differences.

Technology and telecommunications companies can provide digital education programs to their clients, benefitting all parties involved. When someone purchases a cellphone, companies could provide training on privacy settings, how to discern suspicious messages on platforms like WhatsApp, and the importance of safeguarding sensitive information, among other important topics such as those proposed by Twitter and the Organization of American States.

Social media companies also have a role to play in educating users about protecting their identity and reducing cyberattacks. They could create animated and simplified educational videos that users are required to watch before creating an account. Users are already required to review the terms and conditions. Why not add an informative section aimed at teaching the users of the potential dangers that can be found online and what to do in potentially harmful situations? This education would also ensure that users provide informed consent when agreeing to terms and conditions, rather than simply scrolling down and clicking accept.

Latin America still grapples with several challenges in achieving cyber resilience, primarily stemming from limited funding. Small and medium-sized enterprises (SMEs), which comprise 99% of businesses in the region according to the Organization for Economic Co-operation and Development, often lack the financial resources to adequately protect their assets and employ cybersecurity professionals, leaving them susceptible to evolving threats. The ESET Security Report highlights that 65% of specialists acknowledge the need for increased investment in cybersecurity within their organizations. Similar to the above recommendations, governments could incentivize large corporations to offer technical assistance to small businesses at a subsidized rate.

Increasing connectivity and digital literacy will lead to more positive security outcomes in Latin America. By working on this transnational issue together, by educating the population and preparing them for the digital world, we can continue to grow and respond better to cybercrime. We have highlighted some great examples of countries' efforts, but many countries have yet to even make an attempt.

This gap is an opportunity for growth. Countries that struggle with digital literacy levels and cybersecurity preparedness are a blank slate from which they, and the rest of the region, can learn. As a region, we can share our experiences and build upon others' work. A country attempting to increase its digital capacity might take ideas, whether it be specific language or broader lessons, from Peru's National Digital Talent Strategy and Costa Rica's Commission for Digital Government, then adjust them to fit the needs of their country. International collaboration, such as the

Americas Partnership for Economic Prosperity (APEP), spearheaded by the Biden Administration, allows equal partnerships wherein all parties benefit from each other's extensive knowledge.