VP VELOCITY XDR, SYGNIA.

YANIR LAUBSHTEIN

“Organizationally, a mindset shift is required to see cyber risks as operational risks rather than just IT problems”

Digitalisation of water infrastructure improves efficiency, but also increases exposure to cyber risks. Cyberattacks are expected to escalate in frequency, volume, and sophistication, while low awareness and investment result in increased vulnerability of water utilities.

Cristina Novo Pérez

To learn more about the water and wastewater infrastructure cybersecurity trends and readiness in Latin America and the Caribbean (LAC), Source of Innovation, an alliance of the Inter-American Development Bank (IDB) Group with external partners, developed the study *Protecting Water and Sanitation Infrastructure from Cyberthreats: A Cybersecurity Study for Latin America and the Caribbean*. The study author is Yanir Laubshtein, VP of Velocity XDR at Sygnia, one of the leading incident response companies worldwide. In this interview, he discusses the study's main findings on cybersecurity in the water and sanitation sector in LAC.

Please tell us briefly about your career path and how you became involved in the study *Protecting Water and Sanitation Infrastructure from Cyberthreats: A Cybersecurity Study for Latin America and the Caribbean.*

I have more than 20 years of experience working in cybersecurity, with a focus on critical infrastructure and industrial control systems. I started my career in the Israeli Intelligence Corps, where I specialized in cyber operations. I went on to serve as Head of Cyber Security Operations at Israel's Ministry of National Infrastructure, Energy & Water Resources, and later worked as a senior consultant on cybersecurity for water & wastewater utilities and desalination plants under the Israel Water Authority.

My extensive experience securing water infrastructure in Israel led me to become increasingly involved with efforts to improve cybersecurity in the water sector internationally. I served as Director of ICS/OT Cybersecurity at PwC Global Centre of Excellence, advising utilities globally. When the opportunity arose to collaborate on this cybersecurity study for Latin America and the Caribbean, I gladly took the opportunity to lend my expertise to help secure water systems in this critical region. My in-depth knowledge of water sector cyber risks and experience implementing national cyber strategies positioned me well to publish this report.

In my current position, I'm leading Sygnia's (one of the leading IR companies worldwide) Velocity XDR platform, helping our clients to be prepared against cyber-attacks.

> "The water sector faces unique cyber risks due to the nature of water systems and the criticality of uninterrupted service"

What are some of the unique vulnerabilities and risks associated with cyber threats in the water and sanitation sector? Do these vulnerabilities differ from those in other sectors?

The water sector faces unique cyber risks due to the nature of water systems and the criticality of uninterrupted service.

A key vulnerability is the increasing use of industrial control systems (ICS) to remotely monitor and control processes like water treatment and distribution. These ICS use older legacy devices and proprietary protocols that are inherently insecure. They were designed to be isolated, not connected to IT networks. Once connected, they become exposed.

Another critical difference is the potential public health impact of a successful cyberattack. Disrupting drinking water or sewage treatment could quickly endanger public health in ways that distinguish this sector. Environmental contamination is another unique concern.

Unlike some sectors that can withstand brief outages, continuous operability and immediate incident response are crucial for water. Any disruption must be addressed ASAP before services and quality are impacted. The lack of redundancy in water systems also increases vulnerability.

There are also distribution challenges, with huge, dispersed networks of often aging infrastructure spanning vast geographic areas. Securing every access point is difficult. Advanced metering deployments must also be secured.

In addition to all the above, the digital transformation that the sector is undergoing or planned to go through, which involves integrating advanced technologies like IoT sensors and SCADA systems, can increase vulnerability to cyberattacks in several ways as described in the research.

So, in summary, legacy ICS systems, public health risks, lack of redundancy, geographic scale, and a mandate for continuous reliable service create distinct cyber challenges for water utilities.

The report foresees that cyberattacks will escalate in frequency, volume, and sophistication. To what extent is this already a reality in the water sector, and do you think there is a lack of awareness about these threats?

We are already seeing cyberattacks increasing against water utilities worldwide, but I do believe there is still a dangerous lack of awareness and urgency around these threats in the sector.

In the US, cyber intrusions have been detected against several water treatment plants over the past few years. Ransomware is also increasingly impacting municipal water systems - there were over 50 publicly reported incidents against US water facilities in 2021 alone.

While awareness is growing, especially after events like the Oldsmar water plant hack, many utilities still severely underestimate the cyber risks. The technology is often not seen as vulnerable, and attack motivations are not understood. Complacency persists, especially at smaller utilities with limited IT/OT resources. There is much more focus on physical threats.

The lack of strong regulations, oversight, and information sharing on cyber threats contributes to this gap. Utilities often rely on generic IT cybersecurity or vendor guidance lacking sector-specific context. More work must be done to demonstrate the range of motivations, from financial crime to terrorism, and that these threats are both real and escalating. Messages must resonate locally to spur action.

According to the report, most countries in LAC have just started formulating some cybersecurity initiatives involving their critical infrastructure, with some of these strategies already in place. Which findings would you highlight, and did any of them surprise you?

The report's findings on the nascent state of cybersecurity for critical infrastructure in Latin America and the Caribbean unfortunately did not come as a surprise to me.

A few key points stand out:

★ Only 7 out of 32 countries have critical infrastructure protection plans in place. This lack of formal strategy is a significant gap.

★ Most countries are still at an "initial" or "formative" stage of cybersecurity maturity. While efforts are underway, they remain incomplete and disorganized.

★ There is a lack of incentives for public-private cooperation on cybersecurity, which is essential for properly securing privatized critical services like water.

★ Regional collaboration on cybersecurity has been slow to emerge, though organizations like the OAS and IDB are driving improvements.

While these findings are not shocking given the complexity of the challenge, the pace of improvement must accelerate. The threats are escalating faster than defences. A lack of robust governance processes and insufficient technical capabilities present major risks for critical national infrastructure if not urgently addressed. Stronger regulations, funding mechanisms, and international cooperation are needed.

The report also calls for prioritizing and integrating cybersecurity in corporate management and culture. What are the barriers to achieving this, and how can they be overcome?
Achieving true cybersecurity prioritization and integration into organizational culture faces both technical and human challenges.

On the technical side, OT/ICS environments require different tools, controls, and expertise than corporate IT networks. Converging these will take time and investment in skills. Outdated devices lacking security features must also be upgraded.

Organizationally, a mindset shift is required to see cyber risks as operational risks rather than just IT problems. Boards and executives must own and communicate cyber priorities. Competing needs can sideline security. Close coordination is essential between IT, OT/ICS, physical security, and business continuity teams.

Overcoming these barriers starts with leadership setting the vision and tone. Mandating specialized cyber training and bringing in outside expertise help upskill teams. Assessing cyber risks in business terms and simulating incidents make the need real. Integrating cyber into operational metrics and processes embeds security. Significant change takes resources and time, but cultural integration is key for meaningful risk reduction.

"We are seeing cyberattacks increasing against water utilities worldwide, but there is a lack of awareness and urgency around these threats"

How important is considering connections and dependencies between infrastructures within the water and sanitation sector and beyond in cyber protection strategies, and how should they be managed?
Understanding infrastructure interdependencies is hugely important for cyber protection as our systems do not operate in isolation, (although the common misconception of "air gaped")

Within the water sector, connections between treatment, distribution, and wastewater systems create cyber risks that can cascade. For example, a remote terminal unit managing a pumping station could be compromised and allow an attacker to also access downstream treatment systems.

Connections to other critical infrastructures like electricity, transportation and telecoms are also introducing risks if not well secured. Water utilities depend on power for operations, on roads for deliveries, and networks for monitoring. Outages in one can impact others.

Managing this requires several steps:

★ Comprehensively mapping infrastructure and cyber connections (interfaces) between internal systems and external entities.
★ Performing risk assessments of single points of failure that could have outsized impacts.
★ Building in redundancy and network segmentation where feasible.
★ Implementing dedicated monitoring, detection and investigation capabilities that will cover both IT & OT infrastructure, providing holistic visibility and rapid response.
★ Developing coordinated response plans and communication protocols to address multi-system cyber incidents or outages.
★ Fostering closer public-private collaboration on shared cyber risks.

Taking a "systems of systems" approach strengthens resiliency versus addressing sectors in isolation. Cyber planning must consider the cascade effects.

Cybercrime in LAC is defined by regional development fragilities, while water infrastructure that are not digitalised are isolated from many cyber risks. How do the findings for this region compare with the situation in other regions of the world?
The cybersecurity challenges facing Latin America and the Caribbean reflect the region's unique development trajectory and socioeconomic landscape. Several factors distinguish LAC from other parts of the world. As highlighted in the report, high digital penetration combined with lagging cyber governance and law enforcement has created an environment ripe for cybercrime. This distinguishes LAC from less digitized regions.

However, the largely outdated nature of water infrastructure limits risks. In contrast, sectors in Europe and North America are exposing systems to more threats as they modernize. In addition, institutional instability and lack of resources for cybersecurity in parts of LAC are less acute issues in regions like the Asia Pacific and the Middle East. Finally, the concentration of attacks on major economies like Mexico, Brazil and Colombia differs from more dispersed threats in areas like sub-Saharan Africa.

So while cyber crime predominates across higher income regions, LAC's profile is unique. The remaining technology gaps create a paradox - limiting immediate risk but also slowing needed progress on cybersecurity. Stronger regional cooperation and public-private partnerships can help overcome some of these challenges. But improving fundamentals like governance, law enforcement training and infrastructure investment remain critical for LAC to close cyber maturity gaps with other parts of the world.

The responsibility for protecting critical infrastructure is in the hands of both public and private actors, both involved as owners and operators. What should be the role of each of them?

Both the public and private sectors play vital and complementary roles in securing critical infrastructure like water systems. The public sector is responsible for establishing national cybersecurity strategies and policies, designating critical systems, enacting regulations, funding cyber initiatives, and coordinating incident response. Governments must take a system-wide, "macro" view.

Private owners and operators provide the on-the-ground "micro" view into the nuances of operational environments, connected systems, and cyber risks. Their role includes hardening the defences of facilities, adhering to regulations, reporting cyber incidents, participating in industry groups to share threat intelligence, and collaborating with public agencies.

Effective partnerships between the two are crucial. Governments rely on owner/operators' cyber situational awareness and security investments for national resilience. Private companies depend on robust public policy to mandate security and support preparedness through funding, technology, and response capabilities. Alignment and open communication between public oversight and private implementation close capability gaps.

To enhance public-private cooperation, I recommend jointly developing cyber standards and best practices, improving threat data sharing, and establishing councils with both stakeholders for continuous dialogue on improving security programs.

> **Regional collaboration on cybersecurity has been slow to emerge in LAC, though organizations like the OAS and IDB are driving improvements**

Two national models of how governments can protect critical infrastructure from cyber threats, the Israeli and the UK model, are presented; what are the strengths of each and how might they be adapted elsewhere in the world?

The Israeli and UK models offer somewhat distinct approaches with unique strengths that could inform other nations' critical infrastructure cybersecurity.

Israel's model emphasizes centralized oversight and regulation coupled with close public-private sector cooperation. Key strengths include clear guidelines mandating cyber requirements for sectors like water based on risk profiles, which drives action; proactive security reviews and joint exercises with infrastructure operators to validate preparedness; and rapid threat information sharing and coordinated responses to incidents, which speeds reaction.

The UK approach promotes broader cybersecurity ecosystem development and resilience, establishing centres of expertise like the NCSC to lead strategy and incident response. It involves detailed sector-specific strategies like the water cybersecurity guidance, significant funding for cyber skills development and public awareness, and international collaboration to identify threats and shape norms.

Elements of both models could be blended based on a nation's governance model and cyber maturity. The UK's systemic capacity building can complement Israel's hands-on regulatory approach. Joint public-private cyber wargaming, Israel's utilization of cyber regulations, and the UK's public outreach provide examples for adoption globally. Every country has unique risks and resources, but these cases offer tested methods to secure critical systems.