Stepping up defense against cyber threats

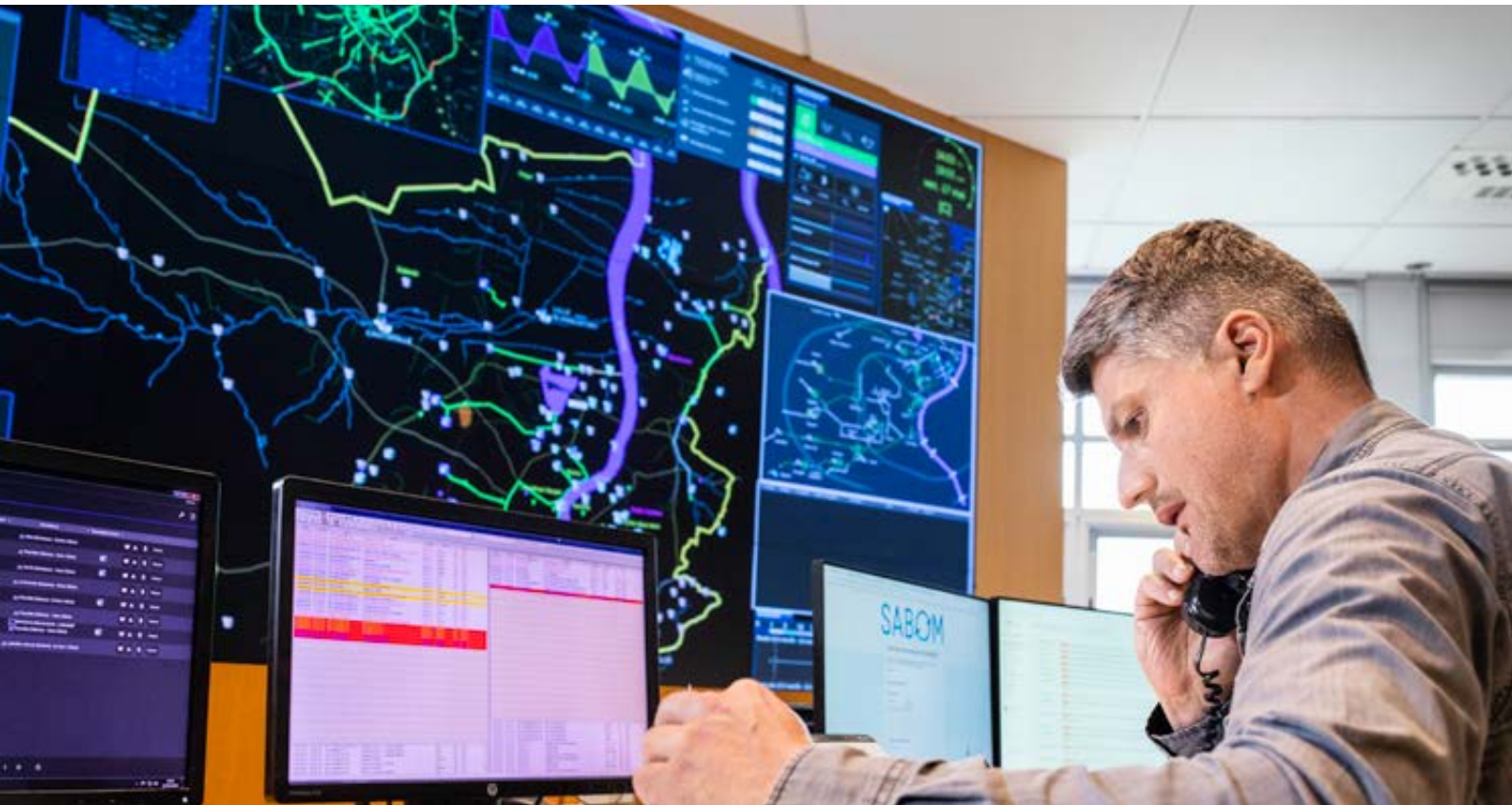
Imagine. It is 3:18 am and everyone for miles around you is fast asleep. You are asleep too. Yet, 5,000 miles away a hacker has gained unauthorized entry to the unsecure system that controls your drinking water infrastructure.

Unbeknown to yourself, the plant manager and the sleeping city all around you, the chemicals that are used by experts to ensure safe and compliant drinking water are being altered.

The chemicals that are used to control the pH of the water and to effectively minimize water pipe corrosion have been increased to deadly levels. And, in just a few hours, the sleepy city will awake to start a brand new day, not knowing that their drinking water is now poisonous.

Now stop imagining. A scenario like this almost happened in February 2021 when an online hacker successfully breached the online system and deliberately tampered with the sodium hydroxide levels at a water treatment plant in Florida, USA, which provides drinking water to more than 15,000 residents of the City of Oldsmar.

The worrying thing about this event is that the vital nature of the water industry makes it a prime target for cybercriminals. The first recorded act of cyber warfare occurred in June 1982 which consisted of a fraudulent modification of the software controlling the



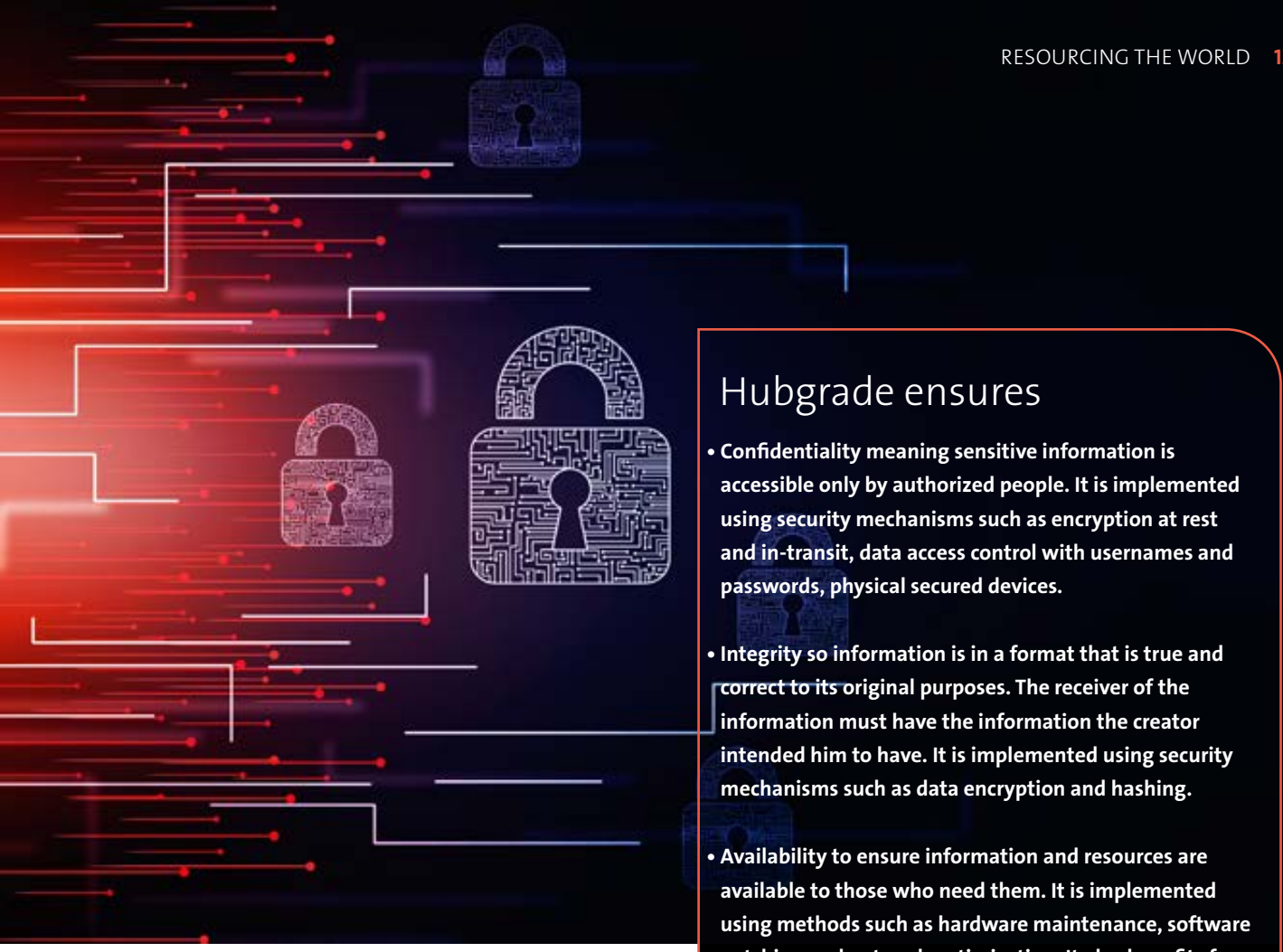
regulation of the pumps, valves and turbines of the trans-Siberian pipeline. This caused the most remarkable non-nuclear explosion ever observed from space.

Since then, cyber attacks have continued to grow in scale. In 2018, the ecosystem of cyber attacks was mainly focused on extortion by small groups or criminal organizations, using ransomware. Nevertheless, geopolitical unrest and cyber terrorism are also important risk factors that should not be minimized. For example, in just one month, May 2019, more than 170 attacks on water infrastructure were recorded in the United States alone.
In 2021, government information security agencies and specialized cybersecurity firms predict an increase in cyber attacks, mainly ransomware attacks targeting critical industries.

"When you consider all of this, it's clear that our number one priority is to offer products with top-notch digital security and compliance," explains Marcelo França, chief information security officer for Veolia's Technology and Contracting division. *"We guarantee a high level of cybersecurity, from the connectivity solution to your industrial control systems to the isolation of application layers. We ensure the protection of our customers' data through a robust access system, a strict encryption policy and innovative means of protection and control that are an integral part of our DNA."*

Our security strategy is based on the fundamental principles of information security which are confidentiality, integrity and availability. Every element of an information security program — and every security control put in place by Hubgrade — has been designed to achieve one or more of these principles.

Our cybersecurity team provides a new driving force from 2021 onwards to meet the challenges we are set to face in the coming years. We are implementing a new strategy, which will enable us to have even greater control to boost our level of cybersecurity and to certify our security management system. We have put in place a cybersecurity academy offering different modules, covering everything from the basics to advanced cybersecurity awareness.



Hubgrade ensures

- **Confidentiality meaning sensitive information is accessible only by authorized people. It is implemented using security mechanisms such as encryption at rest and in-transit, data access control with usernames and passwords, physical secured devices.**
- **Integrity so information is in a format that is true and correct to its original purposes. The receiver of the information must have the information the creator intended him to have. It is implemented using security mechanisms such as data encryption and hashing.**
- **Availability to ensure information and resources are available to those who need them. It is implemented using methods such as hardware maintenance, software patching and network optimization. It also benefits from Amazon Web Services' cloud infrastructure to guarantee high-availability. Dedicated network and web application firewall devices are used to guard against downtime and unreachable data due to malicious actions such as distributed denial-of-service (DDoS) attacks.**

"We will offer guidance to all teams who contribute to the success of our products, including our customers, because we are convinced that everyone is a player in the security business," explains França. *"We are launching an ambitious security modernization strategy based on our experience in the industrial water sector while including the latest international standards in information protection and industrial protection."*

The upcoming years will be an opportunity for us to further develop solutions that are adapted to threats of both the present and the future by partnering with innovative and representative players in the field of cybersecurity.

França adds: *"Without disclosing the content of our strategy, I can mention a few technologies and services, such as micro-segmentation, continuous monitoring of vulnerabilities (Bug bounty), the integration of more security in each brick of the CICD pipeline (DevSecOps) and a rigorous control over the supply chain that will contribute to the success of our system."*

To ensure our mission — to maintain essential water and wastewater services to protect human health and the environment — we require complex and fully connected, flexible systems that can use a constant flow of data from operations and connected production systems to learn, adapt to new demands and benefit from access to expertise.

This requires the processing of secure information (IT) and the implementation of operational systems (OT). *"This infrastructure must be protected at all costs,"* states França. *"And we are prepared to do this. Hubgrade is part of the essential digitization of these new industrial services. We provide our customers with the best tools and expertise to remotely monitor, evaluate and optimize the management of water and energy resources."*