SPOTLIGHT

Cybersecurity

At TTI, we ensure that protecting our customers, employees, and business data meets the highest standards. We have taken the necessary measures to prevent data breaches and enhance our cybersecurity network and digital system. Eduardo Ortiz-Romeu, Global Head of Cybersecurity, oversees the management of data security. Mr. Ortiz-Romeu is a boardroom Qualified Technology Expert (QTE), who specializes in IT, cybersecurity, operational frameworks, and programs that protect organizations' networks, systems, and data.

Mr. Ortiz-Romeu leads TTI's Information Technology Steering Committee (ITSC), which aligns all BUs and helps improve risk and cost management across the Group. The committee meets monthly to review metrics, assess emerging threats and share best practices. We also have a global cybersecurity insurance policy that helps protect us in case of potential breaches.

Cybersecurity conditions are constantly changing, but our programs are designed to continuously assess and develop our security measures. One software program we have in place tracks nearly all 40,000 devices used within the company. This management detection service monitors cyber-attacks and indicators of compromise (IOC), internally and externally, around the clock. Using this system positions the program in a proactive mode against potential cyber-attacks or suspicious activity. We completed the rollout across our global organization in June 2022, with improvements constantly being made. Additionally, we initiated an Operational Technology Assessment in 2022. This assessment evaluated the conditions and risks of our manufacturing and distribution center technology to further enhance the safeguards of our digital and physical assets.

In 2022, one of our key initiatives was increasing employee cyber security awareness and training. We are happy to share our progress on this crucial initiative by launching a monthly cybersecurity training program. The program includes training courses sent to associates with videos designed to be engaging and informative. The training topics include, but are not limited to: password protection, phishing, public Wi-Fi, portable storage devices, and ransomware. Another initiative we expanded is an increased number of regularly sent phishing tests to our employees. This allows us to gauge the effectiveness of our phishing training programs that are in place to help spot potential fraudulent emails and handle them appropriately.

Our completion rate, excluding new hire training, has surpassed the industry average, with a rate of over 80% since the relaunch of the training program. To help motivate our associates we introduced incentive plans to encourage them to complete the training. With these training programs being available to most employees, our objective is to reach 90% completion.

Cybersecurity is an ever-evolving field that requires constant awareness and improvement. As threats to networks, systems, and data continue to emerge and evolve, we must remain vigilant in protecting ourselves. By continuously improving our understanding of cybersecurity and implementing effective governance practices, we can ensure that our organizations are well-equipped to protect against threats and maintain the integrity of our systems and data.

> *"The main goal of our program is to reduce systemic risk across all business units, which allows us to enable growth and remain competitive."*

Eduardo Ortiz-Romeu
Head of Cybersecurity