

LETICIA GAMMILL

FOUNDER AND PRESIDENT OF WOMCY



Since the onset of the pandemic and the massive increase in remote workers, enterprises have been challenged to fully support a hybrid workforce and changes that are being adopted to support it as hybrid work. And if you are in security, your focus can never stop! It's a constantly changing, all-out effort all year long to help your company or organisation #BeCyberSmart.

What are the areas to focus in 2022?

Home networks will continue to be one of the most critical parts of the enterprise network. During the pandemic, malicious remote access attempts grew 2.4 times. In September 2021, the hybrid workforce was targeted with more than 100 million email threats daily according to Cisco's new Hybrid Work Index. I don't expect it to slow down as email continues to be the number one threat vector affecting businesses and users.

Remote employees are working using multiple remote and mobile devices, which expands the threat landscape. Hybrid workers are using multiple devices and connecting directly to the internet to access cloud applications. Work that happened primarily on managed endpoints is now happening on unmanaged ones.

As we continue to see this new hybrid workforce and threat landscape, we also need to pay attention to some other areas that I highlight here:

Supply chain and third-party risk - Attacks like SolarWinds have made

Leticia is the Founder and President of WOMCY, Latam Women in Cybersecurity, a non-profit organisation made up of women, with a focus on the development of cybersecurity. WOMCY's mission is to be a transparent and dynamic organisation that promotes, elevates, empowers and encourages more women into joining the cybersecurity segment. WOMCY has presence in the US and across Latin America and is working to minimise the knowledge gap and increase the talent pool in cybersecurity through its programs in the Education and Corporate segments and Talent development.

headlines in 2021, putting third-party vendor risks front and centre. As we see global supply chain disruptions, this will be an area to watch in the new year.

Vulnerability management – Have a clear direction on how to determine which vulnerabilities pose the highest risk, how they should be tracked and reported to the board. Turn this into a value driver to the business on how to plan for future incidents and build a solid business resiliency strategy.

Talent pipeline – Everyone in security is certainly feeling the effects of security staff shortages which are not slowing down. The importance of programs to increase the talent and diversity pool are more than ever essential at a global level, with a need for the corporate, government and educational sectors to come together with solutions to increase the security workforce.

“

ATTACKS LIKE SOLARWINDS HAVE MADE HEADLINES IN 2021, PUTTING THIRD-PARTY VENDOR RISKS FRONT AND CENTRE.

”