Cyber Security
Industry Advisory Committee

MEDIA RELEASE

Authorised for release by Mr Andrew Penn, Chair of the Cyber Security Industry Advisory Committee

17 November 2021

SECURING A HYBRID WORLD: MANAGING CYBER SECURITY RISKS AS WE EMBRACE A NEW WAY OF WORKING

The Cyber Security Industry Advisory Committee has today highlighted the need to ensure cyber security is managed effectively as businesses shift to hybrid working and outlined practical measures to assist organisations to safely manage long-term hybrid work environments for their teams.

The committee's second thought piece – 'Back to Business: Recognising and reducing cyber security risks in the hybrid workforce' – highlights the key cyber security issues facing Australian businesses – big and small – as the country emerges from the COVID-19 pandemic.

Committee Chair, Telstra CEO Andrew Penn said the positive financial, personal and productivity gains associated with shifting to hybrid work long-term also came with a number of cyber security risks organisations needed to mitigate or manage.

"Hybrid cyber security is now critical and we need to protect infrastructure and data security no matter where it is located," Mr Penn said.

"COVID has forced so many of us to quickly move to remote and hybrid working, which has been transformational and fundamentally changed the way we work.

"This rapid change also means many businesses have been forced to quickly adopt new remote networking solutions, sometimes without appropriate security measures in place.

"As we eye a world beyond COVID restrictions and employees begin to shift from lockdown working to hybrid work arrangements, this is an important moment for organisations to consider how to appropriately secure their infrastructure and their teams' cyber security.

"Cyber security isn't just important for big business; many small and medium businesses have also adopted hybrid and remote working but may have done so quickly and now need to make sure their data and networks are properly secured for a hybrid working future.

"Being cybersafe is also about education. Everyone has a part to play in building a stronger cyber safe environment – at home or at work."

The Committee's thought piece provides practical information and cyber security considerations, including cyber hygiene basics; corporate policy settings; the need for greater training and awareness, and discusses ways to integrate cyber security into business innovation.

"Australia and its cyber infrastructure are under constant attack from cyber criminals, scammers and other bad actors.

"As more of us take up flexible working arrangements, we need to be mindful of securing against these very real threats. If left unchecked, organisations are at risk of cybercriminals gaining access to sensitive data, and disrupting services," Mr Penn said.

Some of the practical steps that both small and big businesses can take to improve their cyber security includes regularly rolling out security patches and making sure software is up to date with the latest releases.

Additional cyber security measures include using multi-factor authentication and device management, securing access to networks by employees who bring their own devices, implementing stronger passphrase and password policies, and ensuring systems are backed up regularly.

"We also need to ensure our people are alert to other risks including using unsecure networks, transferring work files to personal computers, or leaving devices vulnerable in the home or when they're out and about.

"With more people working from home using their own devices, it means individuals and their organisations can be left more exposed to cyber threats due to poor cyber hygiene and digital fatigue, inadequate controls and protections.

"When considering the shift to a hybrid workforce, both private and public sector organisations and their employees need to understand the cyber risks, and ensure correct processes are in place to strengthen their cyber security.

"Whether you're a large corporation, a small business or even an individual who's working more flexibly, this thought piece will help Australians better understand and mitigate the cyber risks of hybrid work by drawing from the Committee's diverse experience," Mr Penn said.

The Industry Advisory Committee's thought piece is available at https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/industry-advisory-committee/papers-and-reports

Media contact: Matt Smithson +61 439 876 981