

Acronis Cyber Readiness Report 2021

Acronis

Regional Deepdive: Asia-Pacific (APAC)

Countries: Australia, India, Singapore

Respondents: 600 IT managers and remote employees

IT managers – Key findings

Despite the infamous attacks on trusted software vendors, like Kaseya or SolarWinds, over half of global IT leaders believe that using “known, trusted software” is sufficient protection – exposing businesses across Asia-Pacific to cyberattacks.

Attacks grow in volume and efficacy

Across APAC region, companies are showing slightly higher numbers of encountered cyberattacks this year.

As for types of attacks, companies in Singapore are facing phishing attacks most frequently, as reported by 74% of IT managers – followed by India at 58% and Australia at 50.5%.

50% of companies in Singapore also faced malware attacks last year, far above the global average of 36% – followed by India at 46%.

Video conferencing attacks have decreased globally since 2020 – yes, still reported by 46% of companies in India, 32.6% – in Australia, and 23% – in Singapore.

Companies in India attacked most frequently – 32% of IT managers report being attacked “at least once a day”, 16% more – “at least once an hour”.

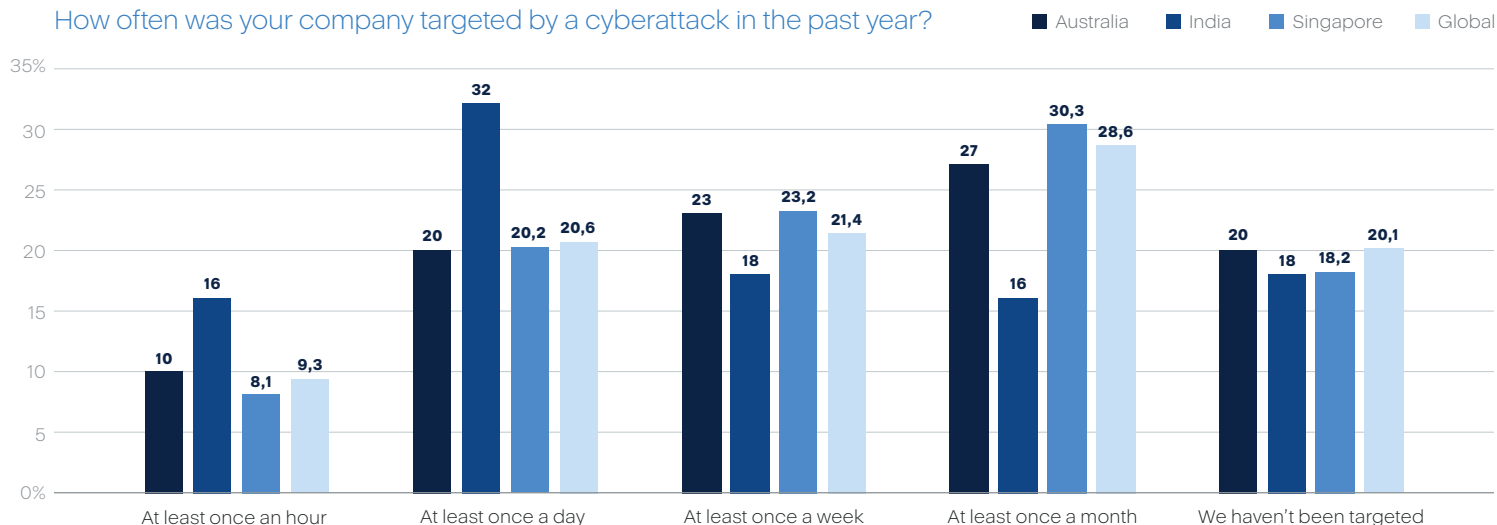
Multi-factor authentication picking up slow

MFA adoption proves lower than expected in APAC – across the region, IT managers are showing reluctance in using the technology, leaving the companies more exposed to phishing attacks among others. Possible reasons for low adoption rates: either the technology seems too complex, or unnecessary, or the most commonly used platforms don't yet offer MFA feature.

India and Australia are showing the lowest adoption rates of MFA technology among IT managers – 50% and 48% of respondents respectively don't use it at all or only use it on some accounts.

Smaller fraction of IT managers uses MFA on all accounts – 26% in Singapore, 21% in Australia and 18% in India.

How often was your company targeted by a cyberattack in the past year?



Remote employees – Key findings

Despite the growing cyberthreats, people will continue to work and hire remotely – that’s the reality all IT teams need to prepare for. Remote employees report hardware shortages, increased software complexity and lack of IT support as the key problems to be solved.

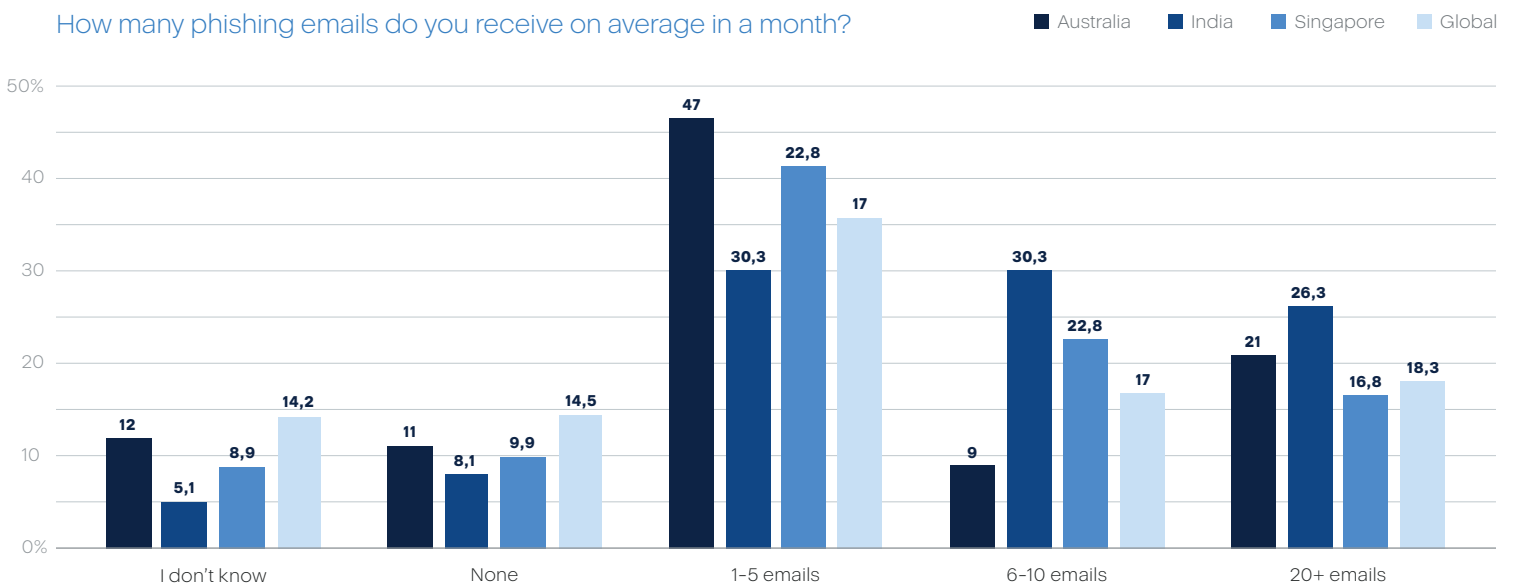
The year of phishing

While detection capabilities, adoption of URL filtering and email security solutions in general have all

increased last year, phishing is still one of the most effective types of cyberattack. Phishing attacks have not only increased in volume, but in sophistication – preying on the human element above all else.

Again, APAC region shows a slight increase compared to global. Remote employees receiving over 20 phishing emails in a month: India – 26.3%, Australia – 21%, Singapore – 16.8%, bringing the APAC average rate to 21.4%, above the global average of 18.3%. While this may suggest better detection tools, extra vigilance is advised for local employees.

How many phishing emails do you receive on average in a month?



The most technically challenging aspects of working remotely / supporting remote work

IT managers	Remote employees
1. Enabling/instructing employees on remote work	1. Wi-Fi connectivity
2. Securing remote workers	2. Inability to use internal network and applications
3. Ensuring availability of corporate apps and networks	3. Difficulty adding new devices to corporate network
4. Software not working properly	4. Using a VPN and other security measures
5. Employees installing unauthorized software	5. Lack of hardware or hardware failure
6. Lack of hardware or hardware failure	6. Lack of IT support

Hardware shortages became a more apparent issue this year globally: employees of giant IT companies globally reportedly have to wait 3 to 6 months for corporate laptops due to chip shortages.

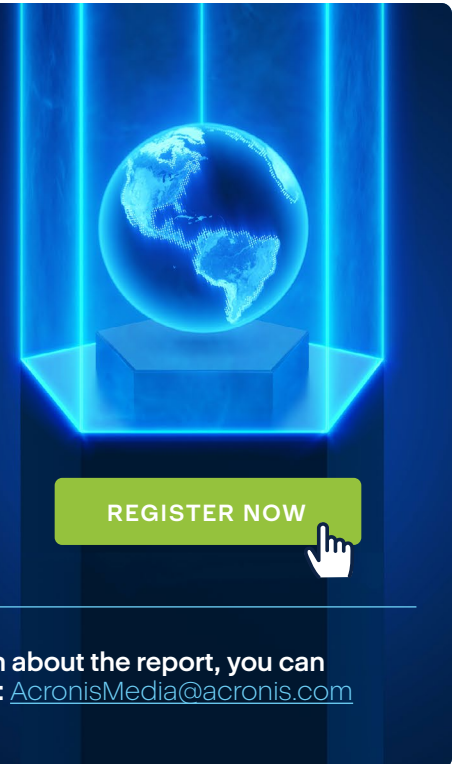
Enabling/instructing employees on remote work proves an extra challenge in Singapore – reported by 68% of IT

managers, the second highest rate among all countries surveyed globally.

67% of remote employees in India reported Wi-Fi connectivity as a top issue – still a top issue second year in a row.

Register now for the Acronis #CyberFit Summit World Tour 2021, kicking off in Miami, Florida on October 25-27, 2021. One platform that allows you to:

- Attend result-focused virtual sessions for free and learn from world-class experts on cyber protection.
- Enhance your MSP business' cyber protection capabilities with advice from the top channel, cybersecurity, and industry experts.
- Hear exclusive case studies of successful, profitable, and scaling MSPs and MSSPs.
- Learn how to grow your business with cybersecurity-forward services.
- Join hands-on, interactive workshops, insightful panels and breakouts, and inspiring keynotes – while enjoying IT channel networking opportunities.



Get access to the recorded sessions from the Acronis #CyberFit Summit World Tour 2021 [here](#)

For more information about the report, you can reach us via email at: AcronisMedia@acronis.com

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated [cyber protection](#) that solves the safety, accessibility, privacy, authenticity, and security ([SAPAS](#)) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, [backup](#), [disaster recovery](#), and endpoint protection management solutions powered by AI. With advanced [anti-malware](#) powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,700 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 25 languages. For more information, visit www.acronis.com

Acronis

Learn more at
www.acronis.com

Copyright © 2002–2021 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and differences from the illustrations are reserved; errors are excepted. 2021-10