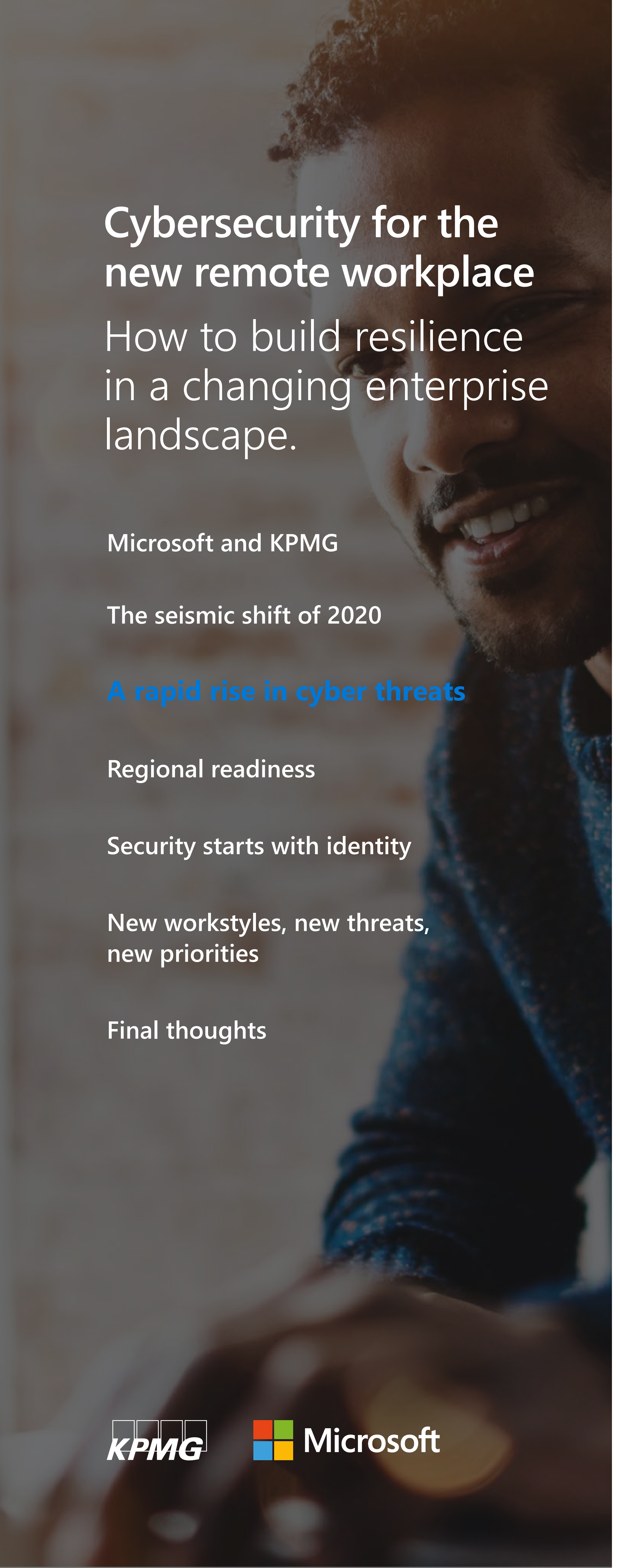

A rapid rise in cyber threats

While the pandemic has brought about a positive spirit of cooperation, collaboration, and resourcefulness across society and business, we have also seen the inevitable flipside—with criminals and opportunists using the pandemic to exploit vulnerabilities.

As the number of employees who work remotely increases, the home IP addresses associated with an organization scales.[4]

> This has expanded the attack surface for criminals, exposing organizations to a diversity of threats such as phishing, fake apps, trojans, backdoors, crypto miners, botnets and ransomware.

Since the outbreak, there has been a reported increase in the volume and sophistication of cybercrimes and cyberattacks conducted by nation states, organized groups and individual hacktivists.[5] Europol has observed that cybercriminals were actively recruiting collaborators in the early weeks of the crisis to orchestrate large-scale phishing campaigns and maximize the impact of their attacks.[6]

As expected, much of this activity is specifically related to COVID-19, with spikes in Coronavirus-related spam. They often employ social engineering techniques, using sophisticated pattern-of-life analyses to entice potential victims to open emails and click on malicious links or attachments.[7] They seek to exploit people's desire for information about the pandemic or to buy goods such as protective masks.

There have also been phishing schemes related to government relief programs in North America and Europe, which attempt to extract bank details from citizens as they apply for financial support payments.[8] Insider threats exist too—ranging from call-center workers cloning customers' card details to investment traders colluding for personal gain, away from the watchful eye of supervisors.[9]

In March, ransomware attacks increased

148%

over baseline levels from February.[10]

In April, Gmail blocked

18M

daily malware and phishing emails, plus more than

240M

daily COVID-19 spam messages.[11]

[4] https://www.bitsight.com/blog/identifying-unique-risks-of-work-from-home-remote-office-networks
[5] https://www.bdo.com.au/BDO_AU/media/Insights/PDF/BDO-Cyber-Threat-Insights-Report-April-2020.pdf
[6] https://www.europol.europa.eu/sites/default/files/documents/report_beyond_the_pandemic.pdf
[7] https://www.mimecast.com/globalassets/cyber-resilience-content/100-days-of-coronavirus-threat-intelligence.pdf
[8] https://fullfact.org/online/coronavirus-phishing-scam/
[9] https://home.kpmg/xx/en/home/insights/2020/05/securing-the-new-reality.html
[10] https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/
[11] https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond