INSIDER INTELLIGENCE | eMarketer

AUG 27
Mack DeGeurin

Big Tech's cybersecurity commitments likely aren't enough to stem rising attacks

Article

The news: Top executives from **Apple**, **Google**, **Microsoft**, **Amazon**, and **IBM** met with US President **Joe Biden** this week to discuss ways the private sector can work alongside the government to bolster national cybersecurity amid a rash of ransomware attacks affecting critical infrastructure, per The Wall Street Journal.

- Though the meeting primarily focused on strategies for mitigating ransomware attacks, it also touched on critical infrastructure security more broadly, supply chain security, and the current dearth of cybersecurity workers.
- Biden called on the tech industry to step up its efforts to bolster defenses, saying “the federal government can’t meet this challenge alone” and calling cybersecurity a “core national security challenge.”

How Big Tech is responding:

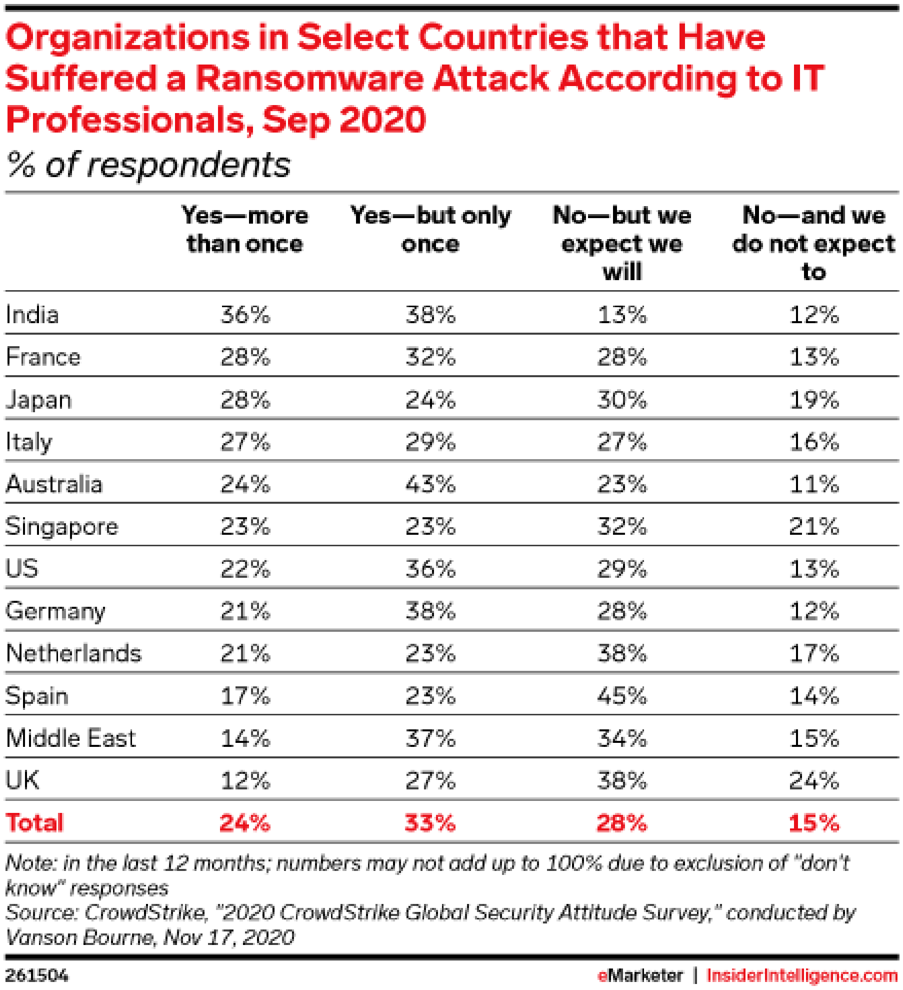
- Microsoft **pledged $20 billion to emphasize security in its product design** and $150 million worth of technical services to help modernize local, state, and federal technology.
- Google plans to **invest $10 billion over five years to bolster its cybersecurity practices** and is committed to training at least 10,000 workers in information technology and data analytics.
- Amazon will provide AWS account holders free multifactor authentication (MFA) devices and will assist other organizations with security training.
- Apple is creating a program to **bolster security within its supply chains** and is working with suppliers to increase MFA adoption.

How we got here: The federal government has faced pressure to step up cooperation with private companies and enact tougher security standards in the wake of last year’s SolarWinds breach and a more recent ransomware attack that briefly forced the world’s largest meat processor to shut down nine plants.

- In July, the administration launched a cross-government ransomware task force aimed at exploring defensive and offensive cybersecurity measures to fend off the growing number of ransomware attacks.
- Around the same time, the president also issued an executive order creating a series of voluntary national security standards that require US agencies to encrypt their data and use two-factor identification. The administration is reportedly considering making these requirements mandatory.

The takeaway: Though commitments made by executives after the meeting signal meaningful forward motion that may alleviate some security pressure at the margins, it will likely do little to stem the tide of escalating ransomware attacks.

- Instead, the federal government needs to pass legislation or put more aggressive executive orders in place mandating security standards that are enforceable with a threat of penalties.
- Any effective security policy will likely require greater cooperation between local governments, which are some of the most vulnerable targets of ransomware attacks.



Organizations in Select Countries that Have Suffered a Ransomware Attack According to IT Professionals, Sep 2020

% of respondents

	Yes—more than once	Yes—but only once	No—but we expect we will	No—and we do not expect to
India	36%	38%	13%	12%
France	28%	32%	28%	13%
Japan	28%	24%	30%	19%
Italy	27%	29%	27%	16%
Australia	24%	43%	23%	11%
Singapore	23%	23%	32%	21%
US	22%	36%	29%	13%
Germany	21%	38%	28%	12%
Netherlands	21%	23%	38%	17%
Spain	17%	23%	45%	14%
Middle East	14%	37%	34%	15%
UK	12%	27%	38%	24%
Total	**24%**	**33%**	**28%**	**15%**

Note: in the last 12 months; numbers may not add up to 100% due to exclusion of "don't know" responses
Source: CrowdStrike, "2020 CrowdStrike Global Security Attitude Survey," conducted by Vanson Bourne, Nov 17, 2020

261504 eMarketer | InsiderIntelligence.com