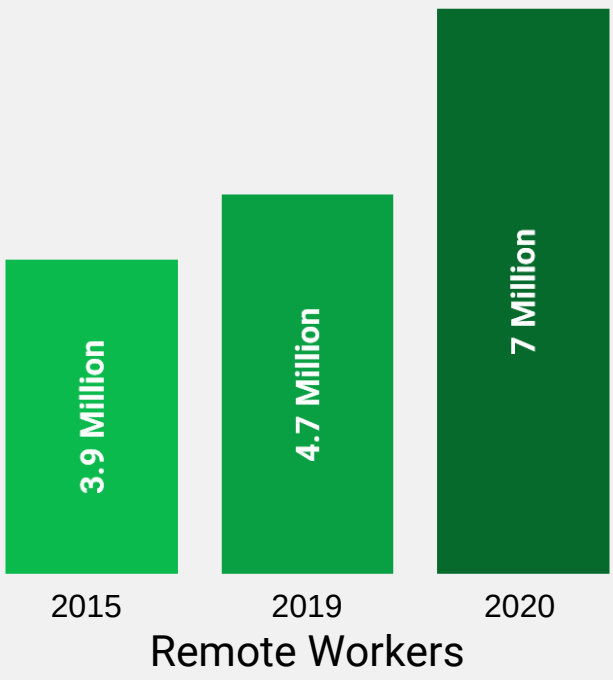
Cybersecurity in the Post COVID World

What You Need to Know



Remote Workers Increase Threat Landscape

The massive transition to working remotely exposed unknown vulnerabilities that greatly impacted organizations. Increased remote access to private data instantly increased the threat landscape, giving cyber criminals new territory to exploit.

36 billion private records exposed in 2020

Increase in Cyber Crime

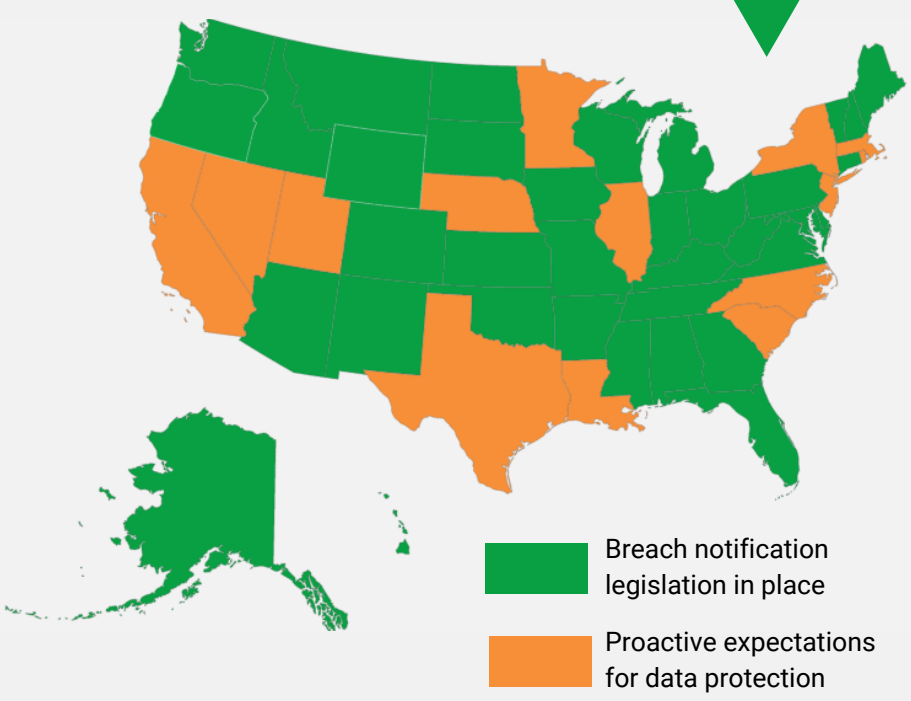
Cyber criminals took full advantage of the whirlwind the pandemic caused. Unprotected remote workers proved easy targets, causing a rapid rise in attacks.

Increase in Regulations

As cyber crime escalated, states and industry regulators increased their timelines and expectations toward cybersecurity. By 2022, almost every business will be touched by a compliance expectation from their state, industry or contracted vendors.

Increase in Cybersecurity and Privacy Regulations

Increase in fines and penalties for non-compliance



States are increasing expectations on

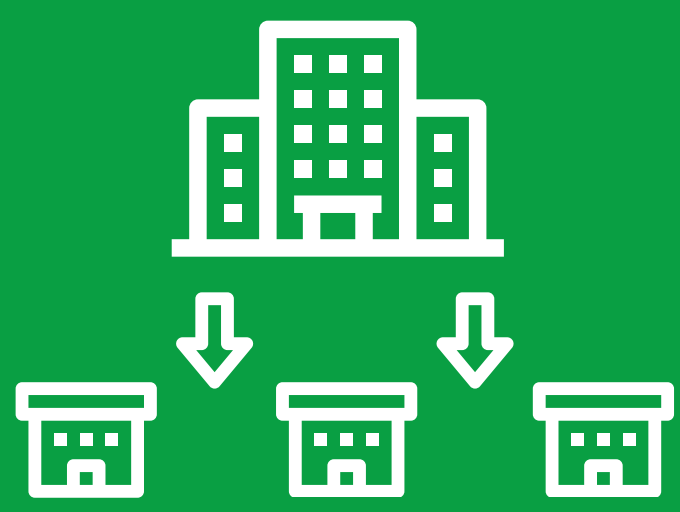
- ✓ data protection
- ✓ data disposal
- ✓ breach notifications

While state expectations for protecting data vary widely, we are seeing a trend in more states implementing proactive data protection legislation.

Trickle Down Effect

As state and industry regulations increase fines and penalties, vendor compliance expectations also expand. Big businesses are requiring their vendors to get compliant or risk losing contracts.

CMMC escalated these expectations by requiring all DoD vendors to earn a certification in order to win contracts.



Cyber Resilience is the Path Forward

Post-Covid world has taught us that building cyber resilience is the best way for your business to survive and thrive with these new threats that go across your business ecosystem.

Start building cyber resilience today, before you are attacked, miss a contract opportunity or get fined.

CyberCompass®

Navigating You to Cyber Resilience