CROWDSTRIKE

WORK SECURITY INDEX

SECURING THE REMOTE WORKFORCE IN COVID-19

COVID-19 has forced many companies to quickly transition to remote work, while cybersecurity challenges have increased as adversaries prey on fear and disinformation to launch cyberattacks. YouGov in conjunction with CrowdStrike surveyed organizations globally to determine security risks during this time.

GLOBALLY

56%

of respondents are working from home more often as a result of COVID-19

60%

of respondents are using personal devices while working remotely

89% OF GLOBAL RESPONDENTS BELIEVE THAT THEIR DEVICES ARE SECURE AGAINST ADVANCED CYBER THREATS

50% OF RESPONDENTS BELIEVE THAT THEIR BUSINESS IS ROUGHLY THE SAME OR LESS LIKELY TO EXPERIENCE SERIOUS CYBERCRIME IN THE WAKE OF COVID-19, YET CROWDSTRIKE HAS CONFIRMED A 100X INCREASE IN COVID-19-THEMED MALICIOUS FILES FROM FEBRUARY TO APRIL 2020

53% OF RESPONDENTS GLOBALLY ADMIT THAT THEIR COMPANY HAS NOT PROVIDED ANY ADDITIONAL CYBERSECURITY TRAINING ON THE RISKS ASSOCIATED WITH REMOTE WORK

LARGE ORGANIZATIONS	MEDIUM-SIZED ORGANIZATIONS	SMALL ORGANIZATIONS
33%	43%	69%

CROWDSTRIKE RECOMMENDS SIX KEY FACTORS THAT CAN HELP ENSURE REMOTE WORKER CYBERSECURITY:

- Update your current cybersecurity policy to include remote working.
- Implement a secure access plan for BYOD on corporate networks.
- Prepare for sensitive data being accessed via unsecured networks.
- Maintain cybersecurity hygiene and comprehensive visibility into endpoints.
- Continue cybersecurity training as coronavirus-themed scams escalate.
- Prepare crisis management and incident response plans to be executable by a remote workforce.

Survey Methodology:
CrowdStrike commissioned YouGov plc to conduct an online survey of 4,048 senior decision makers in Australia, France, Germany, Great Britain, India, Japan, Netherlands, Singapore and the U.S. Fieldwork was undertaken April 14-29, 2020.