

Healthcare and finance industries aren't securely transferring data over mobile devices



Due to the COVID-19 pandemic, more employees than ever in the healthcare and finance industries are working remotely. While many of these organizations have implemented secure file sharing systems at the office, remote workers using mobile devices can't always access them—and are frequently defaulting to unencrypted email.

Progress and Pulse surveyed over 100 security leaders in these two industries to determine how they're securing mobile file transfers as employees use unencrypted technologies.

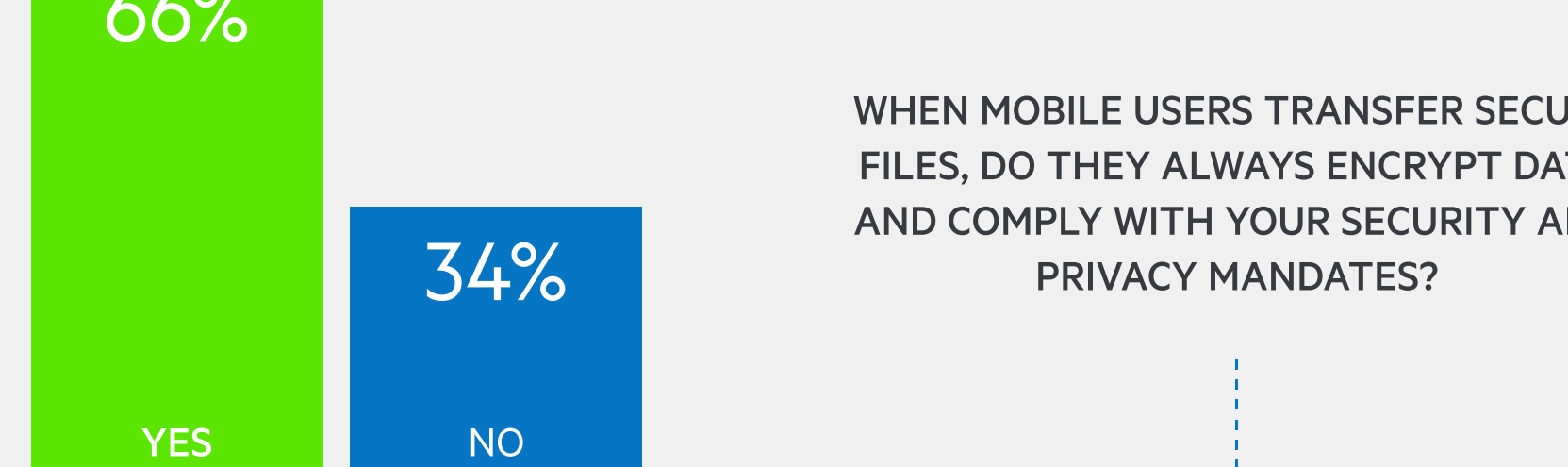
Data collected from May 20 - June 10, 2020

Respondents: 108 security executives in the healthcare and finance industries

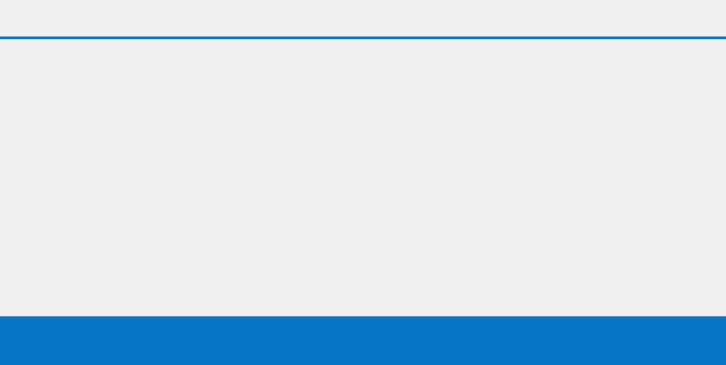
MOST SECURITY LEADERS SAY CONFIDENTIAL MOBILE FILE TRANSFERS ARE SENT THROUGH EMAIL

Email is an inherently insecure medium for file transfers and does not support large files or any type of tamper-evident log. However, it is still being used regularly to transfer secure files. An incredible 70% of healthcare organizations say they send secure files—like patient records and insurance claims—via email. Finance professionals reported a slightly better email usage of 51%, but in both industries only a minority were using secure file sharing tool.

HOW MANY USERS SEND SECURE FILES THROUGH EMAIL?



Despite the vast majority of confidential files being sent through email, 66% of security leaders believe their employees always encrypt data and comply with security and privacy mandates.



WHEN MOBILE USERS TRANSFER SECURE FILES, DO THEY ALWAYS ENCRYPT DATA AND COMPLY WITH YOUR SECURITY AND PRIVACY MANDATES?

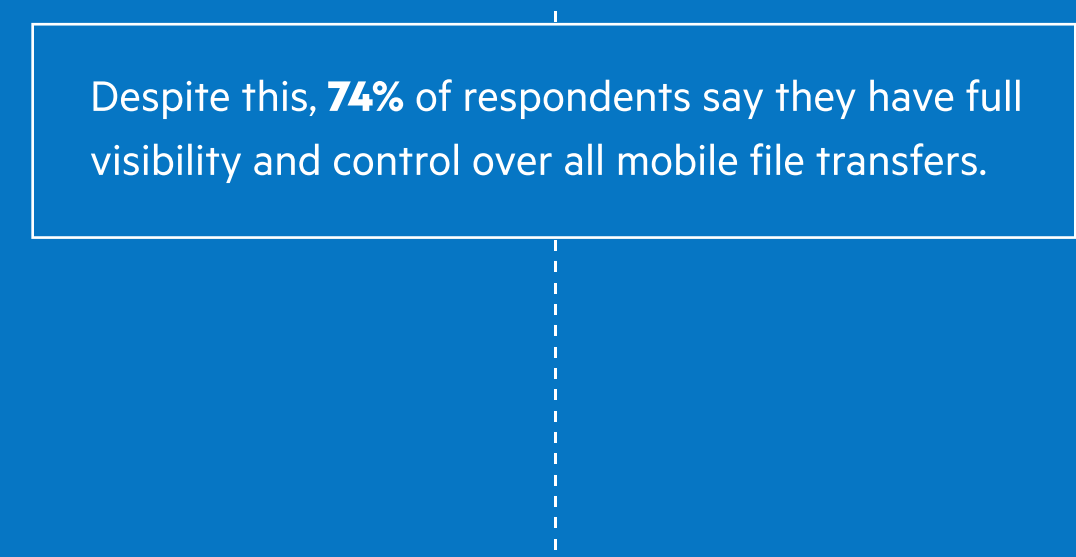
Executives in the finance industry are more certain their company's mobile file transfers are encrypted than those in the healthcare space.



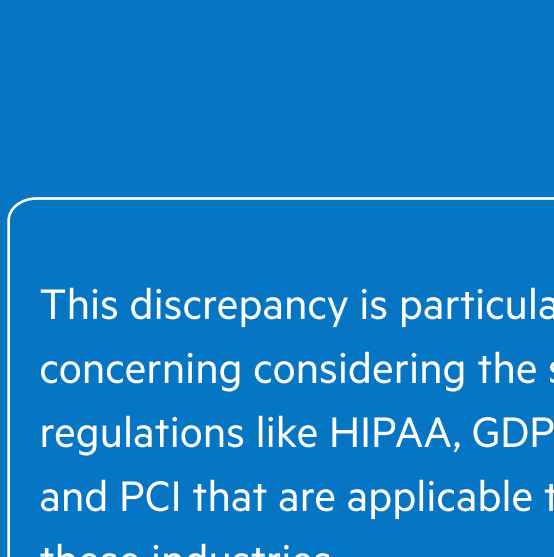
SECURITY LEADERS SAY THEY HAVE FULL VISIBILITY OVER FILE SHARES, BUT ONLY 9% CAN REPORT ON ALL MOBILE TRANSFERS

Considering the percentage of email being used, it's not surprising that 91% of tech execs can't report on and audit all mobile file transfers that occur at their organizations.

WHAT PERCENTAGE OF ALL SECURE FILE TRANSFERS OVER MOBILE DEVICES CAN YOU REPORT ON AND AUDIT?



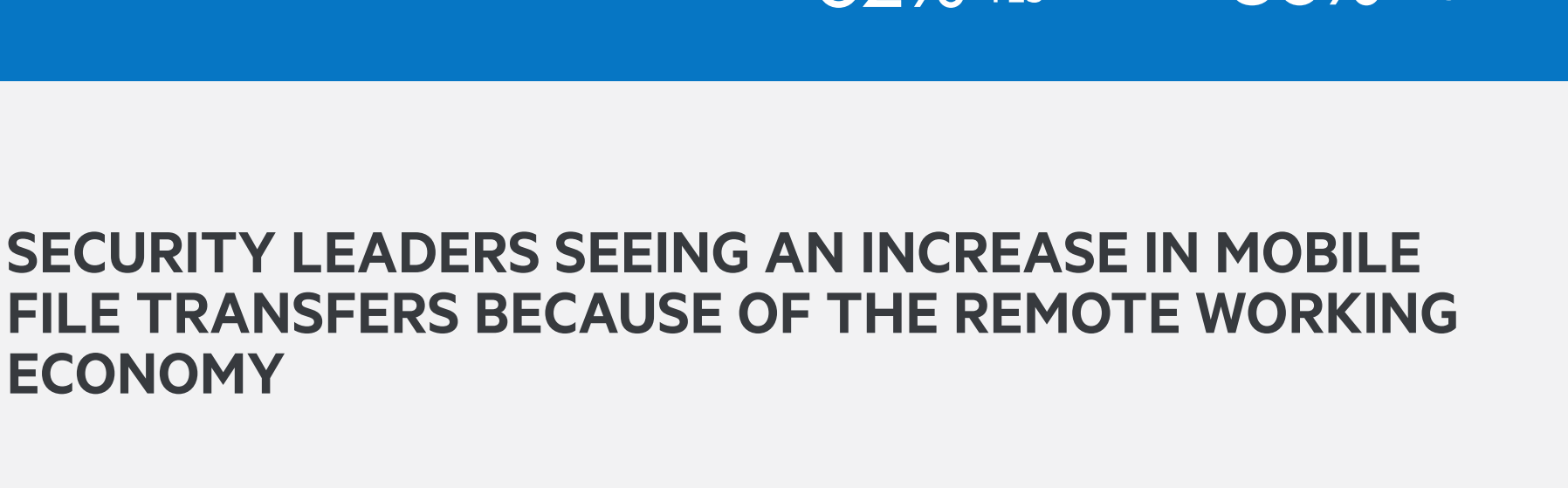
DO YOU HAVE FULL VISIBILITY AND CONTROL OVER ALL MOBILE FILE TRANSFERS AT YOUR COMPANY?



Despite this, 74% of respondents say they have full visibility and control over all mobile file transfers.

By industry, finance and insurance companies are more confident in their visibility than healthcare organizations.

ARE YOU CERTAIN MOBILE FILE TRANSFERS ARE ENCRYPTED?

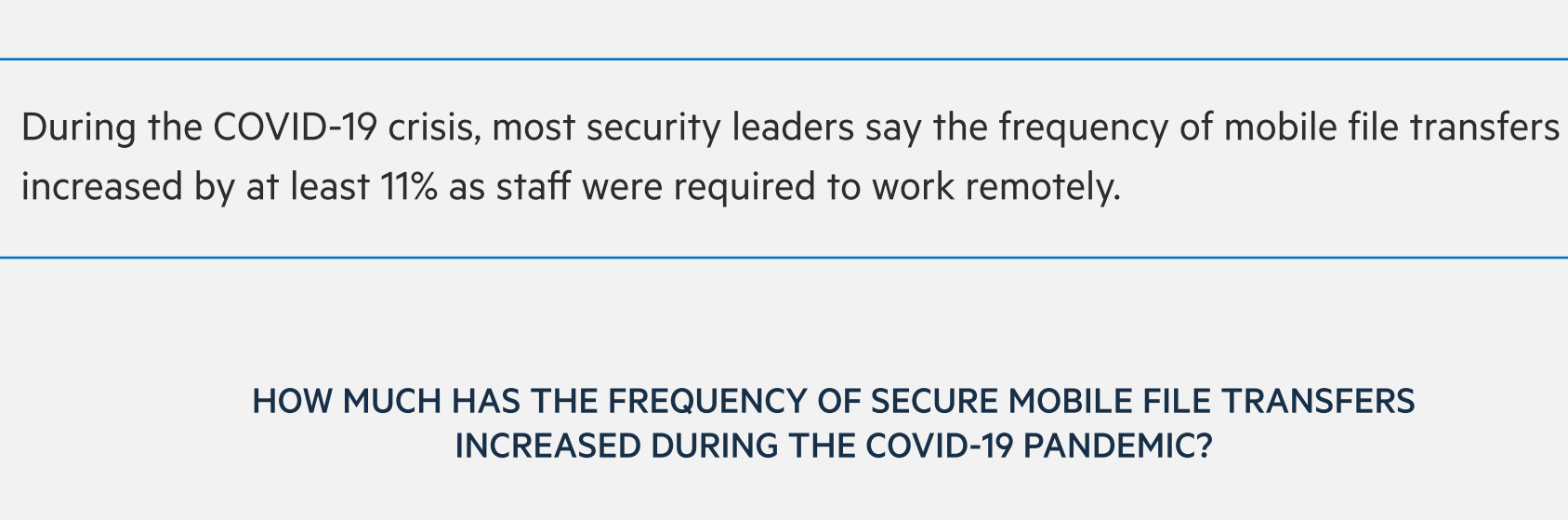


This discrepancy is particularly concerning considering the strict regulations like HIPAA, GDPR and PCI that are applicable to these industries.

SECURITY LEADERS SEEING AN INCREASE IN MOBILE FILE TRANSFERS BECAUSE OF THE REMOTE WORKING ECONOMY

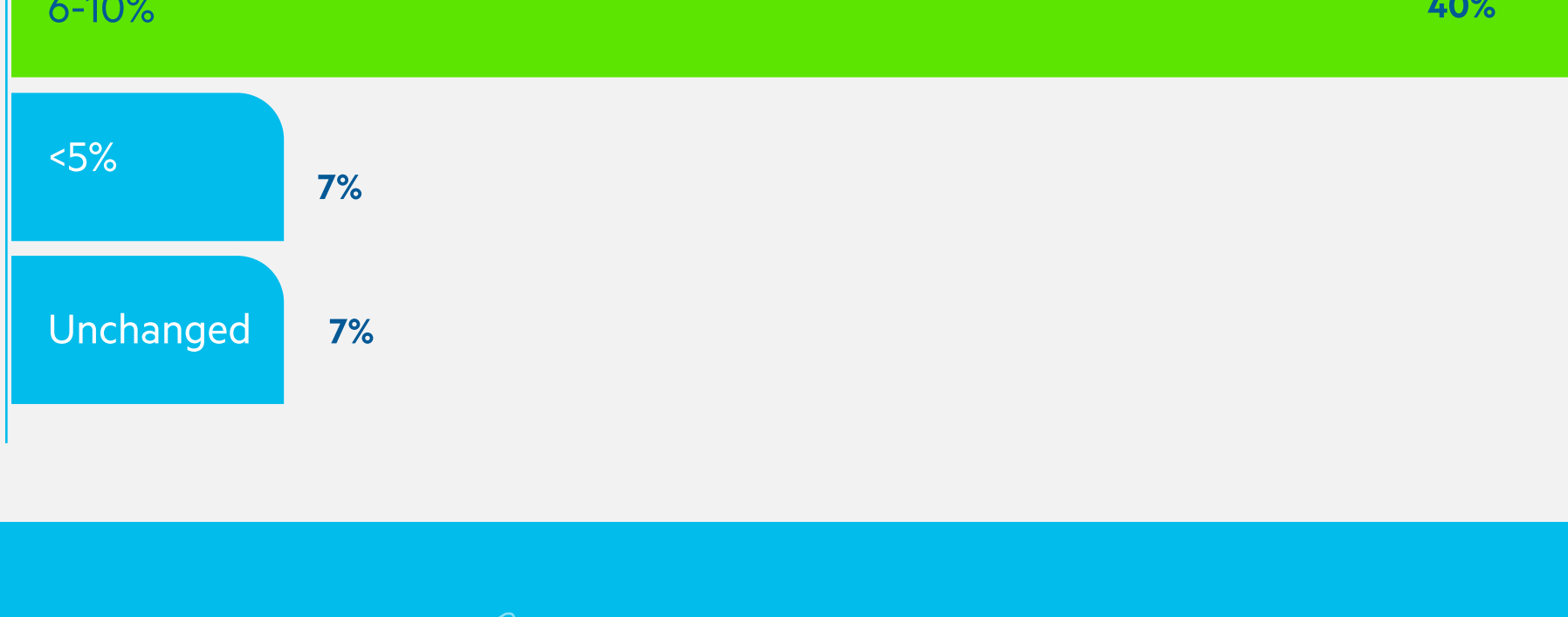
Most executives estimate 11-15% of secure file transfers originate from mobile devices today.

WHAT PERCENTAGE OF ALL SECURE FILE TRANSFERS ORIGINATE FROM A MOBILE DEVICE AT YOUR ORGANIZATION?



During the COVID-19 crisis, most security leaders say the frequency of mobile file transfers increased by at least 11% as staff were required to work remotely.

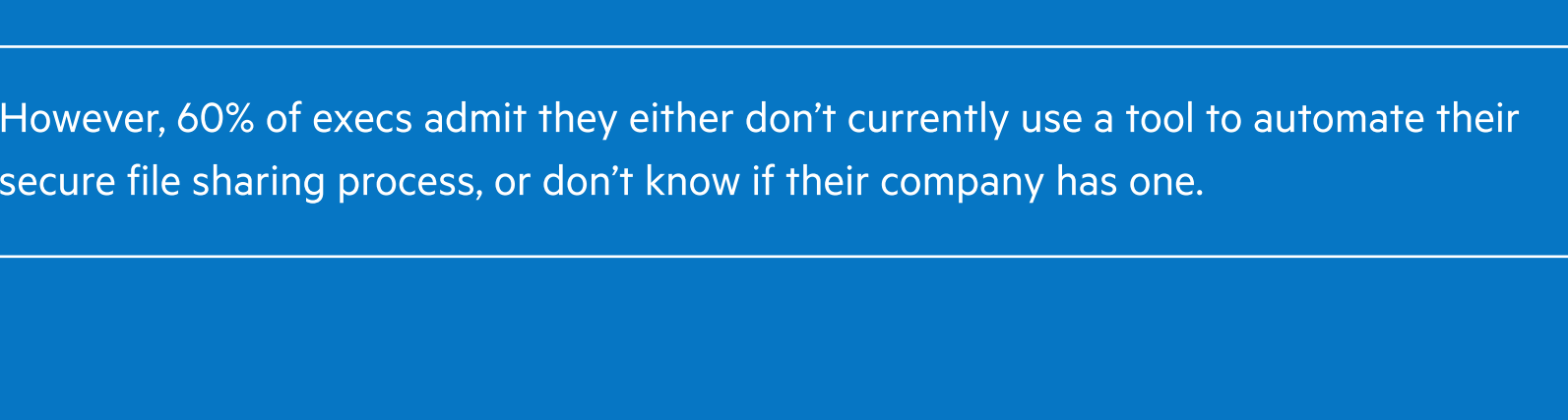
HOW MUCH HAS THE FREQUENCY OF SECURE MOBILE FILE TRANSFERS INCREASED DURING THE COVID-19 PANDEMIC?



However, only 22% of mobile users can fully access the same file sharing systems they can use on-premises.

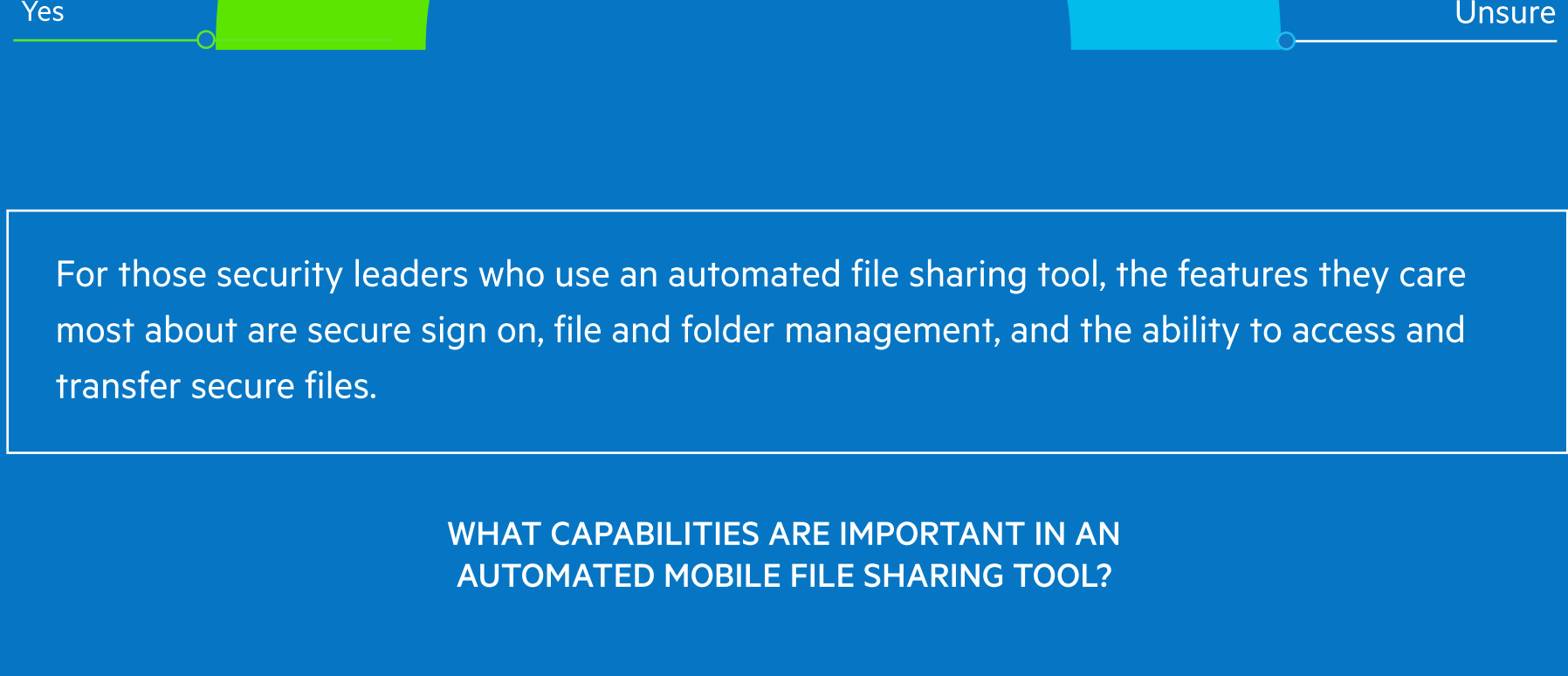
MANUAL FILE SHARING AFFECTS EFFICIENCY AND THE BOTTOM LINE, BUT ONLY 40% HAVE AN AUTOMATED FILE SHARING TOOL

91% of security leaders agree that sending secure files manually depletes efficiency and detracts from their company's bottom line.



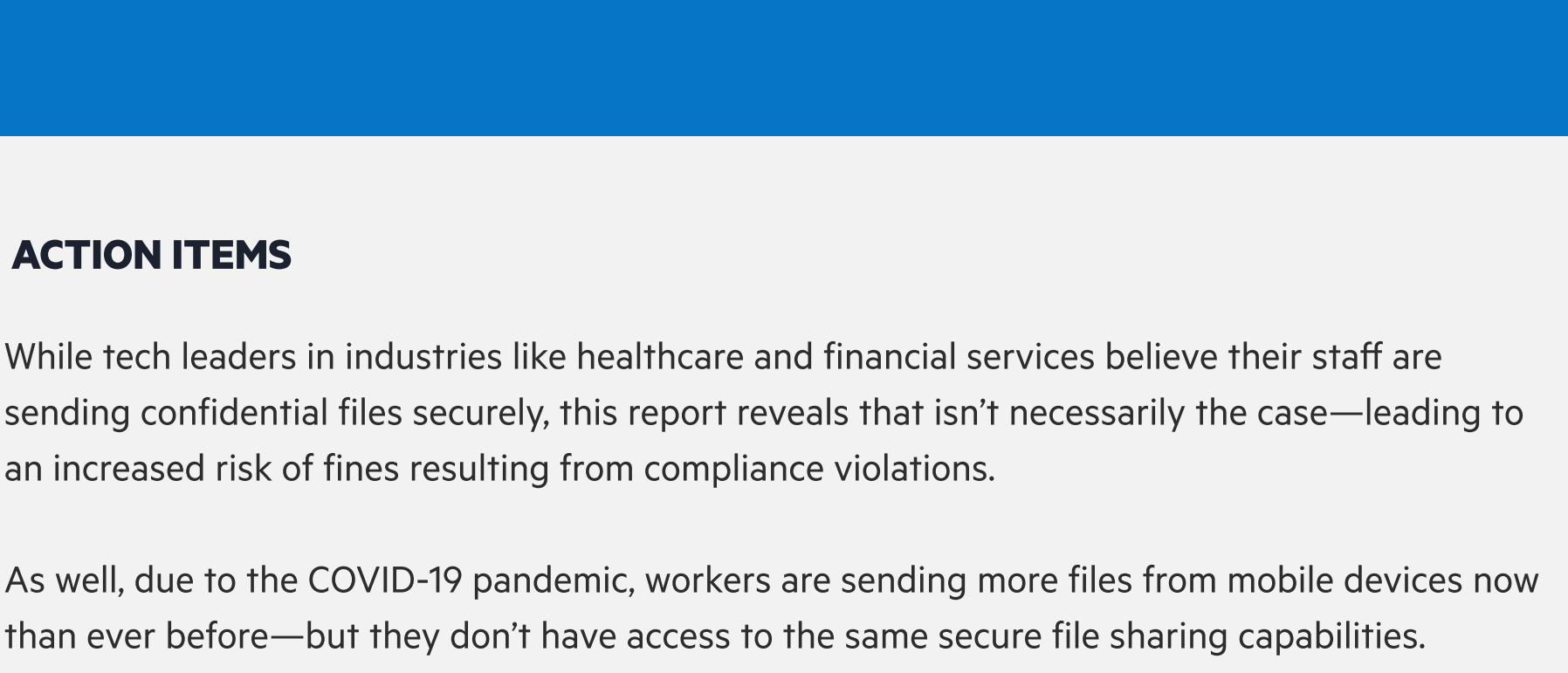
However, 60% of execs admit they either don't currently use a tool to automate their secure file sharing process, or don't know if their company has one.

HAVE YOU AUTOMATED CONFIDENTIAL FILE SHARING WITH SOFTWARE?



For those security leaders who use an automated file sharing tool, the features they care most about are secure sign on, file and folder management, and the ability to access and transfer secure files.

WHAT CAPABILITIES ARE IMPORTANT IN AN AUTOMATED MOBILE FILE SHARING TOOL?



ACTION ITEMS

While tech leaders in industries like healthcare and financial services believe their staff are sending confidential files securely, this report reveals that isn't necessarily the case—leading to an increased risk of fines resulting from compliance violations.

As well, due to the COVID-19 pandemic, workers are sending more files from mobile devices now than ever before—but they don't have access to the same secure file sharing capabilities.

To increase efficiency, reduce the risk of human error, and prevent fines, leaks, PR damage, and lawsuits, these organizations should consider secure, managed file transfer solutions that provide:

- Robust, tamper-evident audit logging
- Real-time reporting and visibility
- A simple, full-featured mobile app
- A powerful automation engine

Respondent Breakdown

Location



Company Size



Industry



Title

