VERITAS

Ransomware

Paying hackers is a losing game.



of consumers believe that hacked companies should stand up to cybercriminals



of consumers demand compensation from the company if they can't

and refuse to pay ransoms.

restore their data.



\$1,167

per affected person is the average ransom consumers believe companies should pay to retrieve their data.



of consumers would stop using the company's services no matter what it decided.

Demanding sanctions against CEOs.



of consumers blame CEOs personally if their companies are breached by ransomware.





want the CEO to pay a fine.

demand a prison sentence.

demand the CEO be banned from running a company in the future.

demand the CEO resign.

want the CEO to take a pay cut or be demoted.

ask for a public apology.

Back up, don't pay up.







of consumers expect companies to implement security software to protect their data.

624

of consumers expect companies to have tried-and-tested backup copies of their data.



These steps allow companies to ward off ransomware attacks or at least restore data after an attack without paying a ransom.

For more information about data protection visit www.veritas.com/protection/ransomware-protection

VERITAS



Methodology: Interviews conducted and statistics compiled for Veritas Technologies LLC by 3Gem. A total of 2,000 consumers were interviewed in April 2020 in each market (China, France, Germany, Japan, United Kingdom and United States) adding up to a global sample size of 12,000 adults over the age of 18.

Copyright © 2020 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and Backup Exec are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. V1053 6/20