Ransomware

Paying hackers is a losing game.

71% of consumers believe that hacked companies should stand up to cybercriminals and refuse to pay ransoms.

65% of consumers demand compensation from the company if they can’t restore their data.

$1,167 per affected person is the average ransom consumers believe companies should pay to retrieve their data.

44% of consumers would stop using the company’s services no matter what it decided.

Demanding sanctions against CEOs.

40% of consumers blame CEOs personally if their companies are breached by ransomware.

42% ask for a public apology.

35% want the CEO to pay a fine.

30% demand the CEO be banned from running a company in the future.

27% demand the CEO resign.

25% want the CEO to take a pay cut or be demoted.

23% demand a prison sentence.

79% of consumers expect companies to implement security software to protect their data.

62% 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.

Back up, don’t pay up.

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.

40% of consumers believe that hacked companies should stand up to cybercriminals and refuse to pay ransoms.

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