UK SURVEY
DECEPTION TECHNOLOGY: PLAYING CYBERCRIMINALS AT THEIR OWN GAME

November, 2017

Fidelis™ Cybersecurity

Deception technology: playing cyber criminals at their own game

"As organisations move toward proactive network defence, we're seeing the rapid emergence of automated detection and deception technology. This turns the table on the often-used social engineering tactics of attackers.

"With this, breached organisations can either revoke the attacker or take matters into their own hands, launching retaliatory strikes to recover any stolen data and avoid, for instance, having to pay a ransom to decrypt sensitive files.

"With respondents in the UK showing such support for the legalisation of retaliatory strikes and decreasing confidence in the data protection strategies of organisations and the government, I'm sure we will be watching what happens in America with great interest. Put simply, it might take playing attackers at their own game to keep future intrusions at bay."

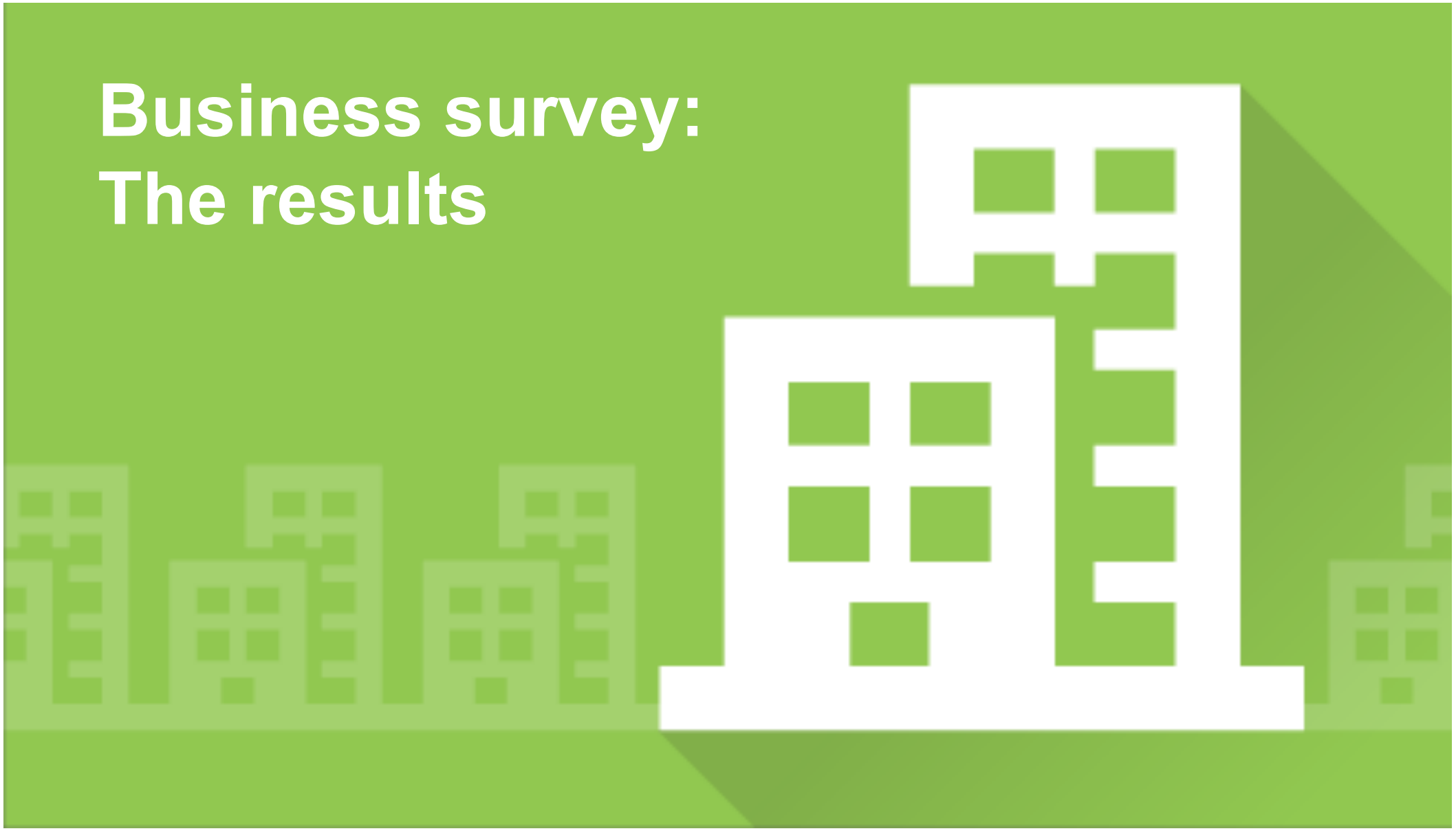
Andrew Bushby, UK Director at Fidelis Cybersecurity

Survey overview

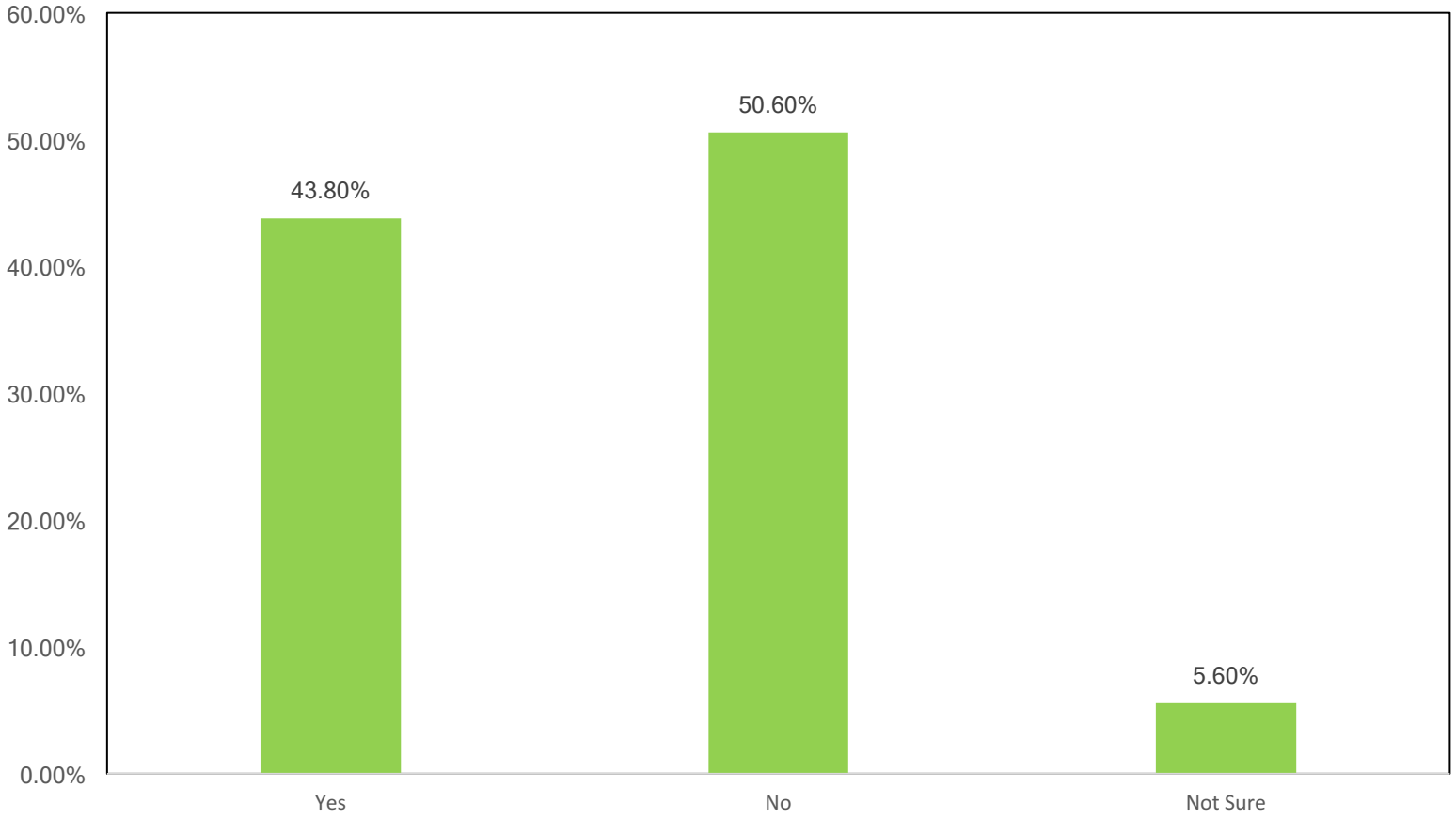
The aim of this survey was to explore the attitudes of British consumers and organisations towards a move from defensive to an offensive security posture, specifically ‘hacking back’ – a topic that has become globally significant due to ongoing discussions in US Congress over its legislation. The study suggests that there is a definite appetite to evolve UK defence strategies in line.

The survey was conducted by 72Point in November 2017, targeting 500 business professionals and 2,000 consumers across the UK.

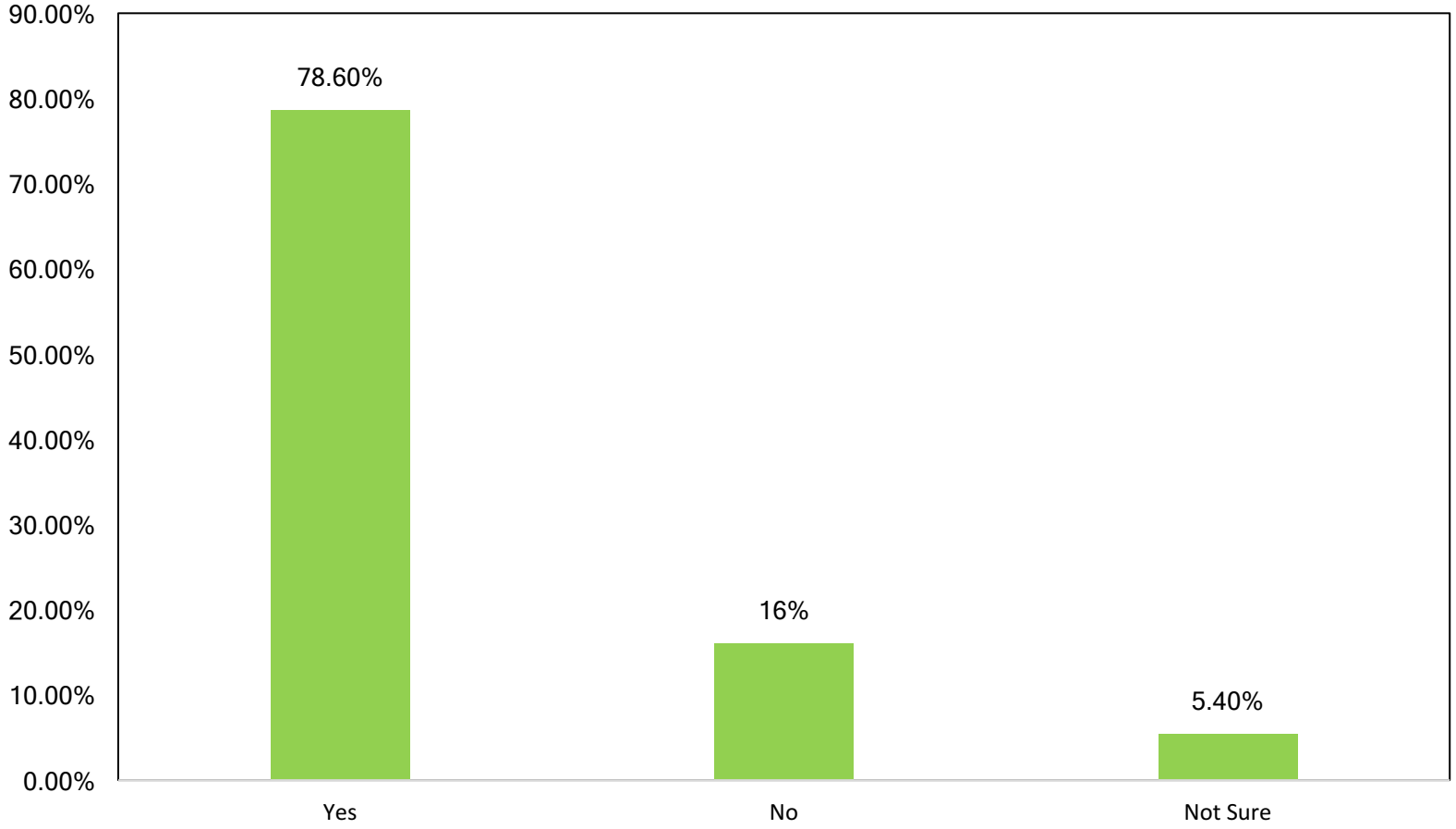
Business survey: The results



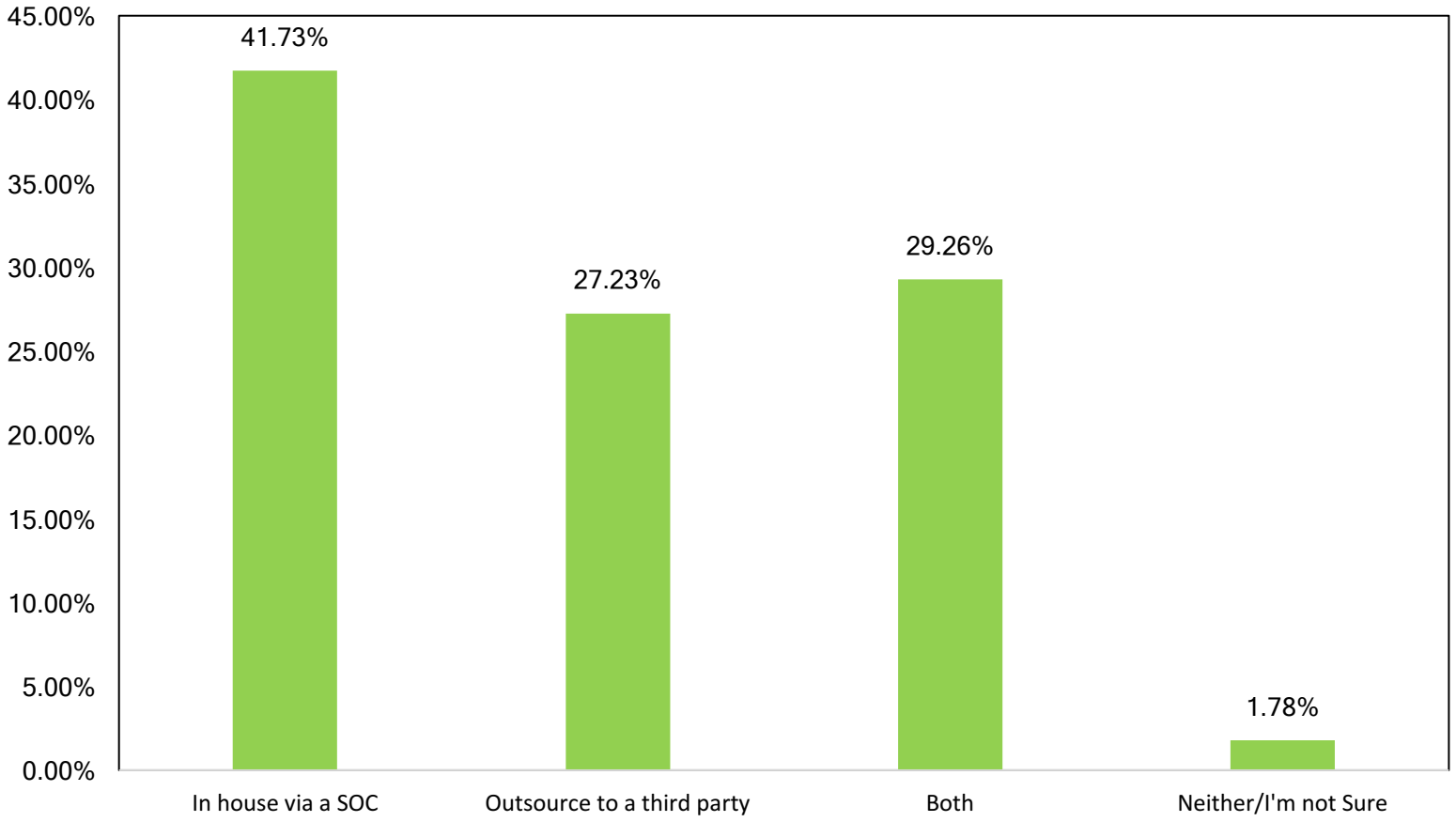
Has your organisation every suffered a data breach as a result of a cyber-attack?



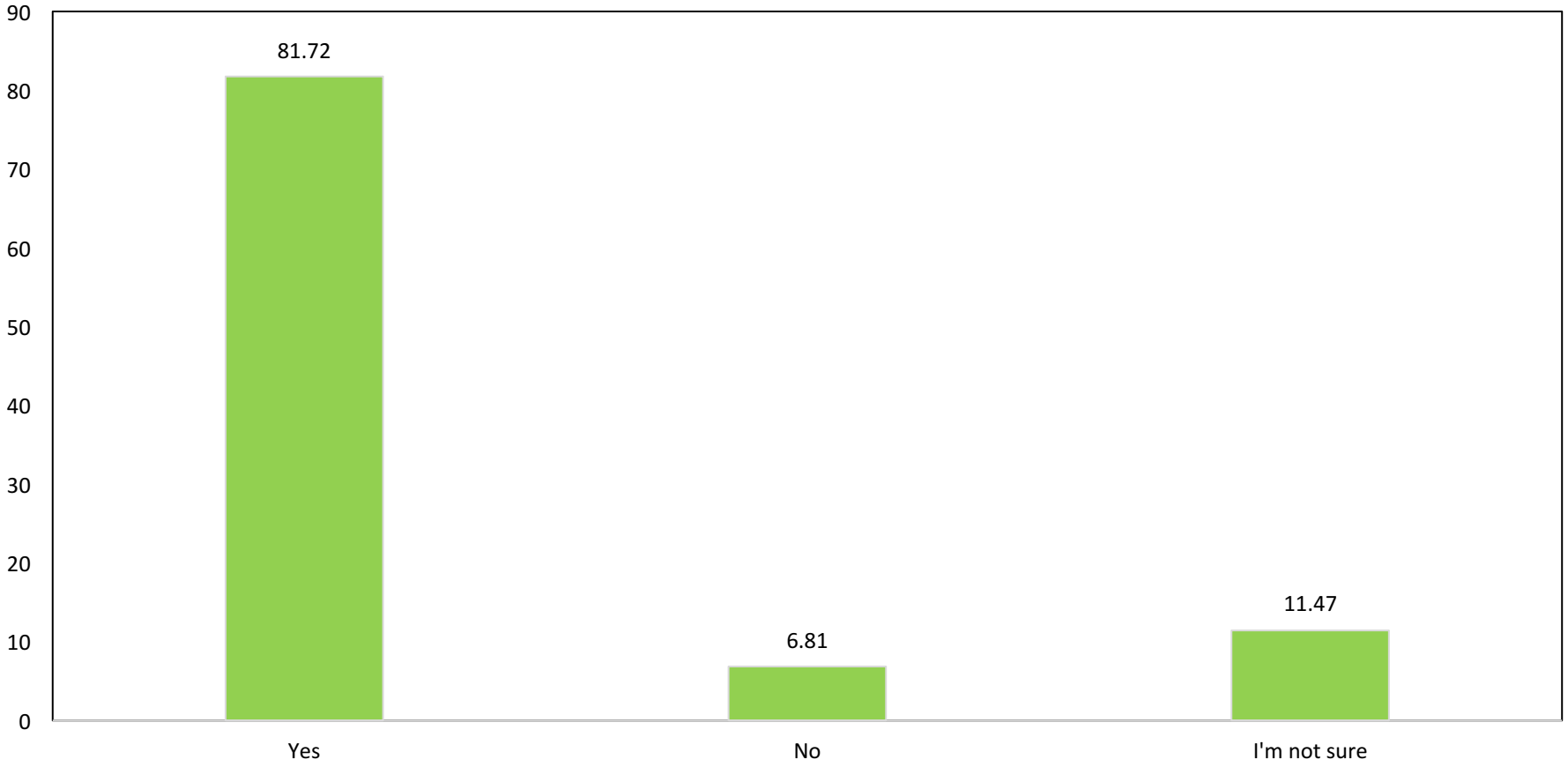
Do you have a strategy in place in case of a data breach?



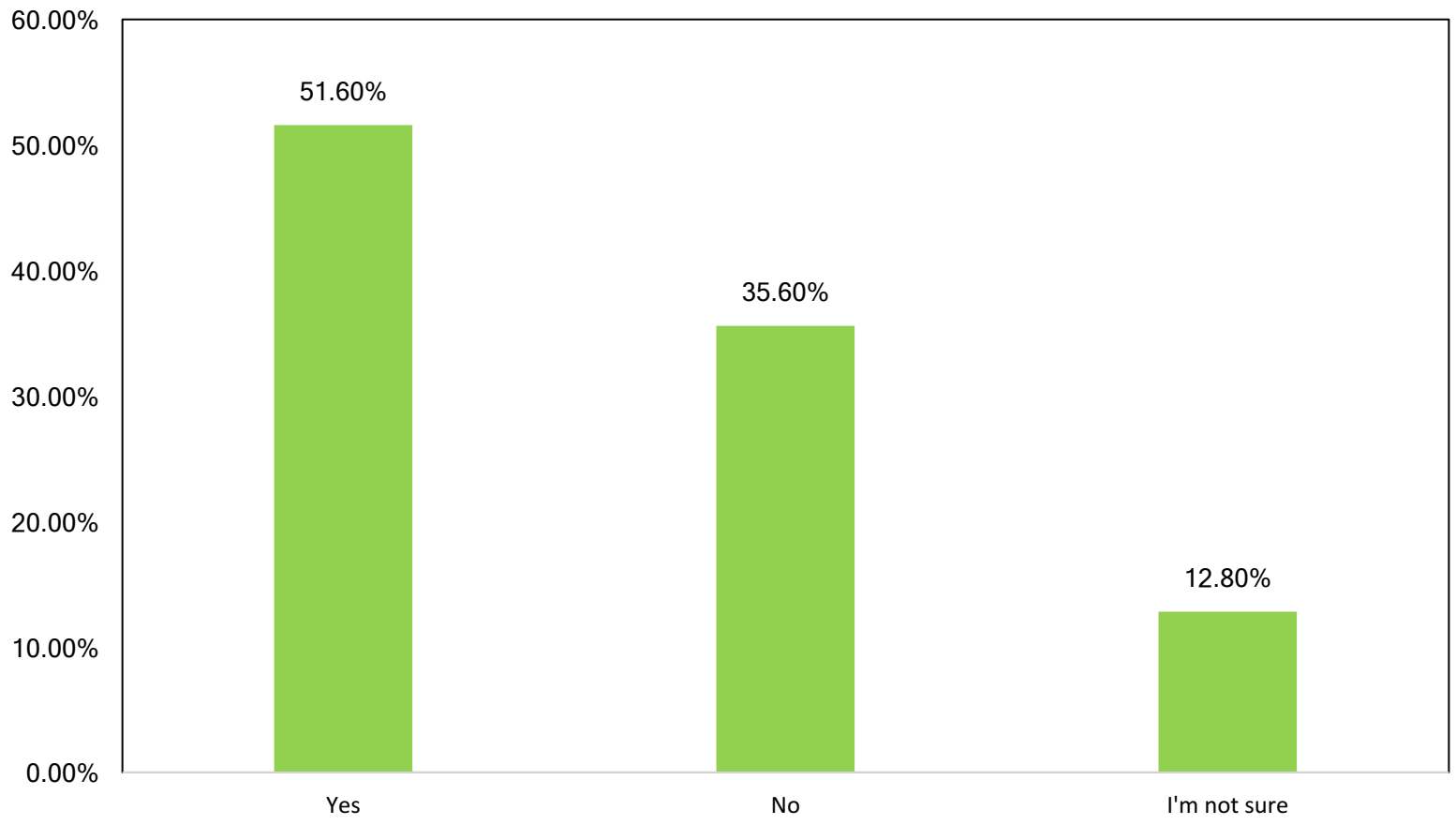
Thinking about your breach strategy, do you manage your security provision in house via a Security Operations Centre (SOC), or outsource to a third party?



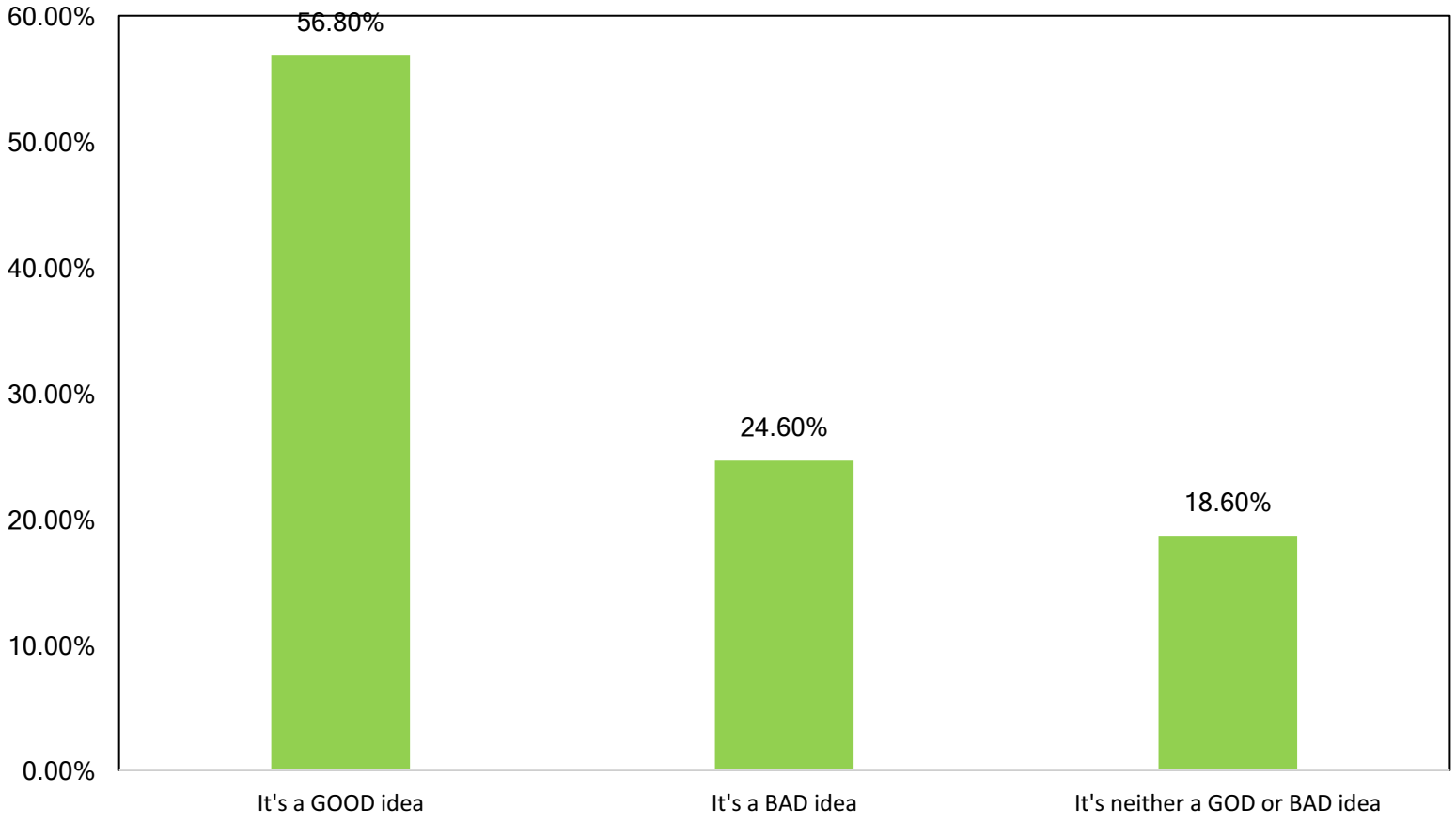
If you manage your security in-house, do you think that your company would benefit from automating your detection, prevention and response?



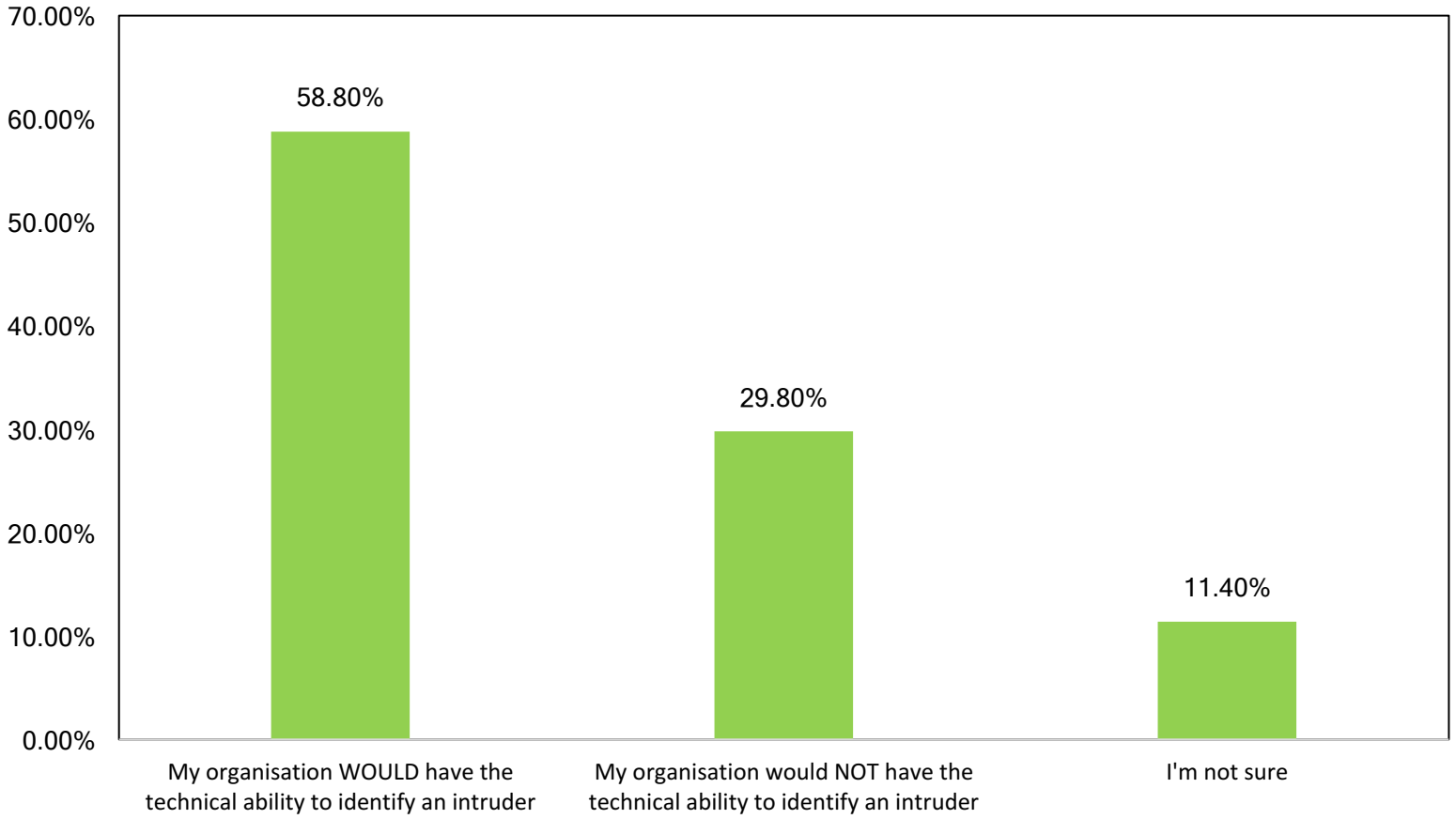
In your organisation, do you have an offensive security policy that enables you to minimise damage after a breach or to recover stolen data?



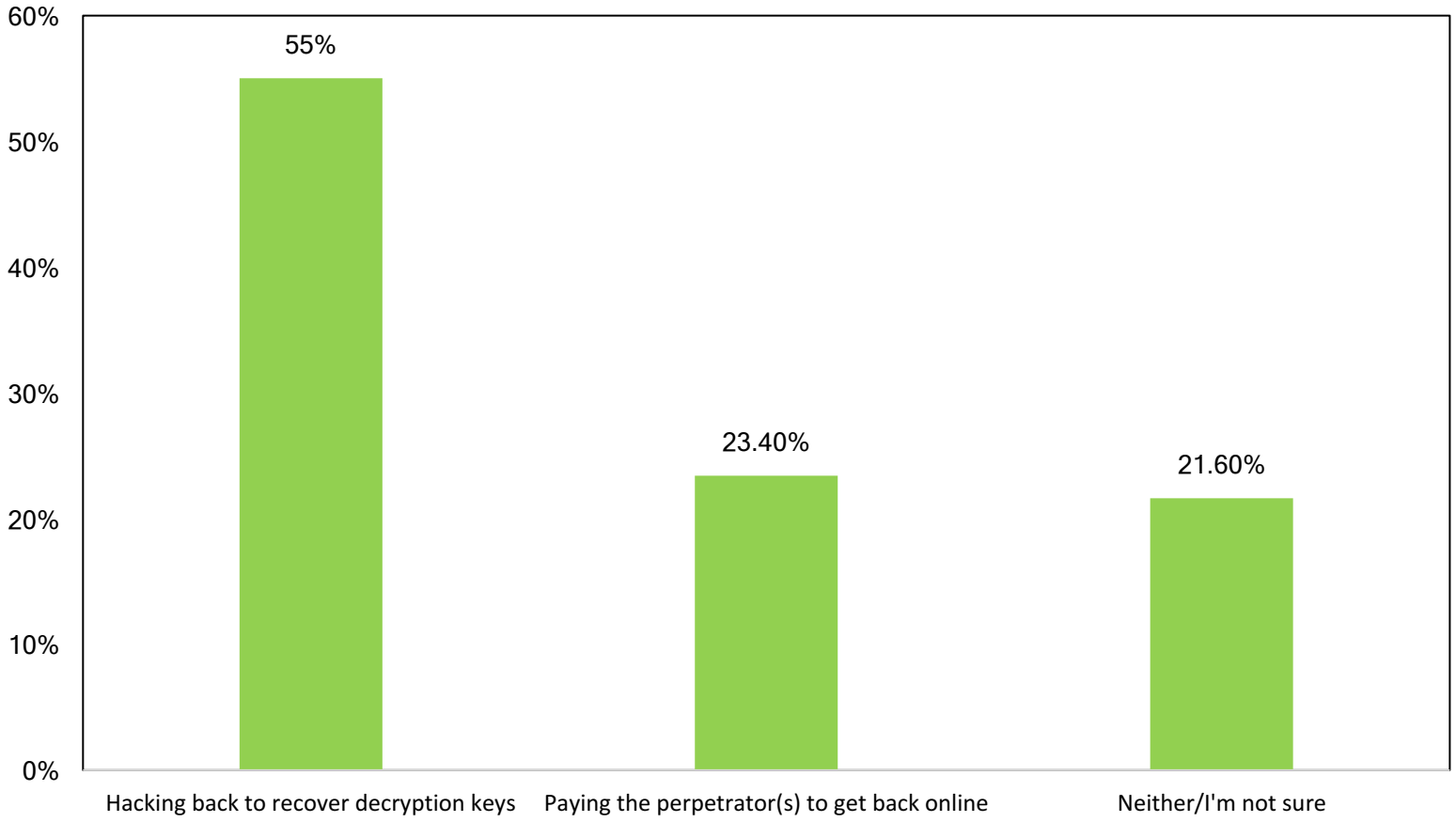
In regards to organisations and ‘offensive security,’ which of the following best describes your opinion?



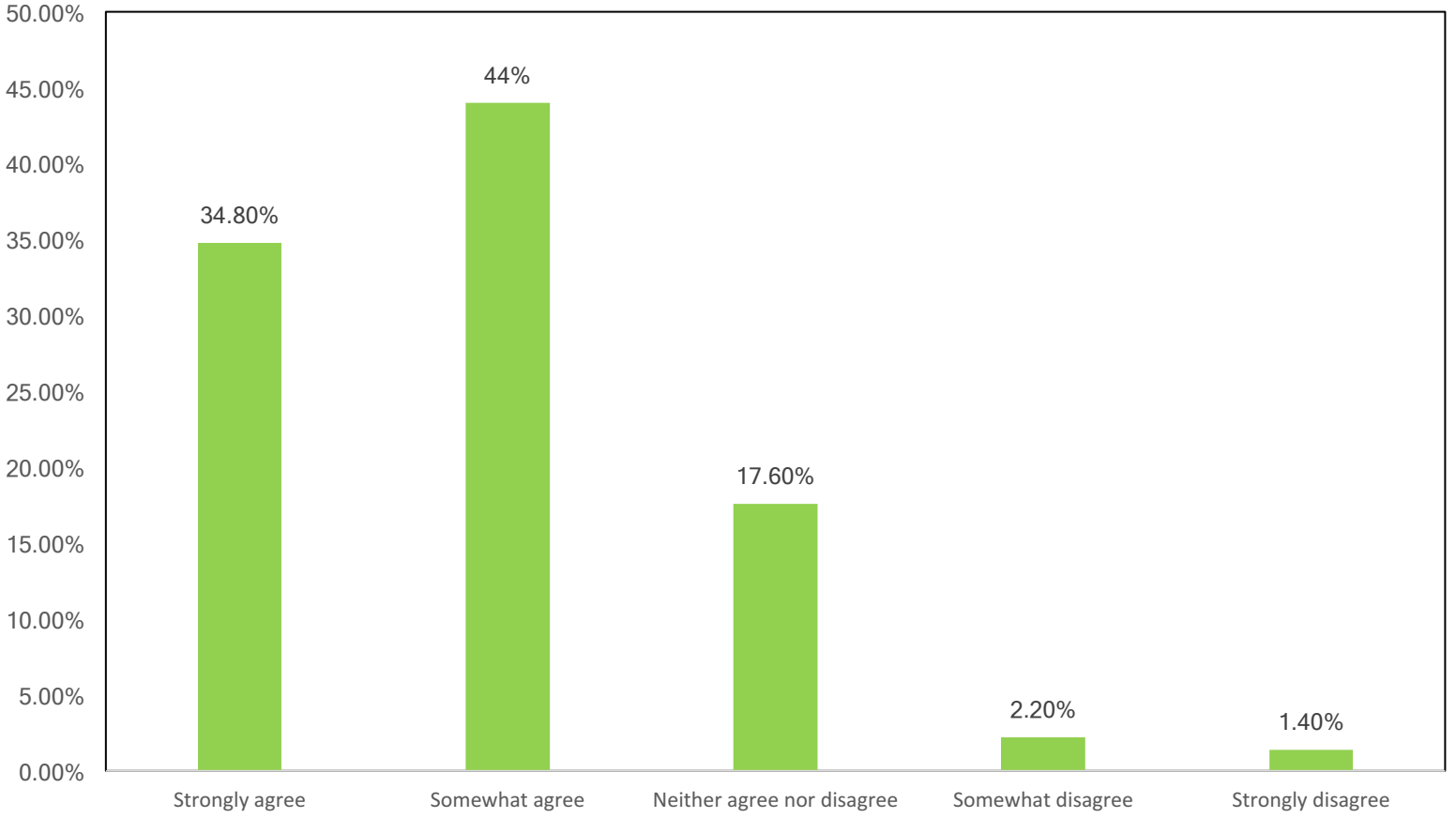
In regards to having the technical ability to identify an intruder, infiltrate their systems and destroy any data that had been stolen after a cyber attack, which of the following applies to your organisation?



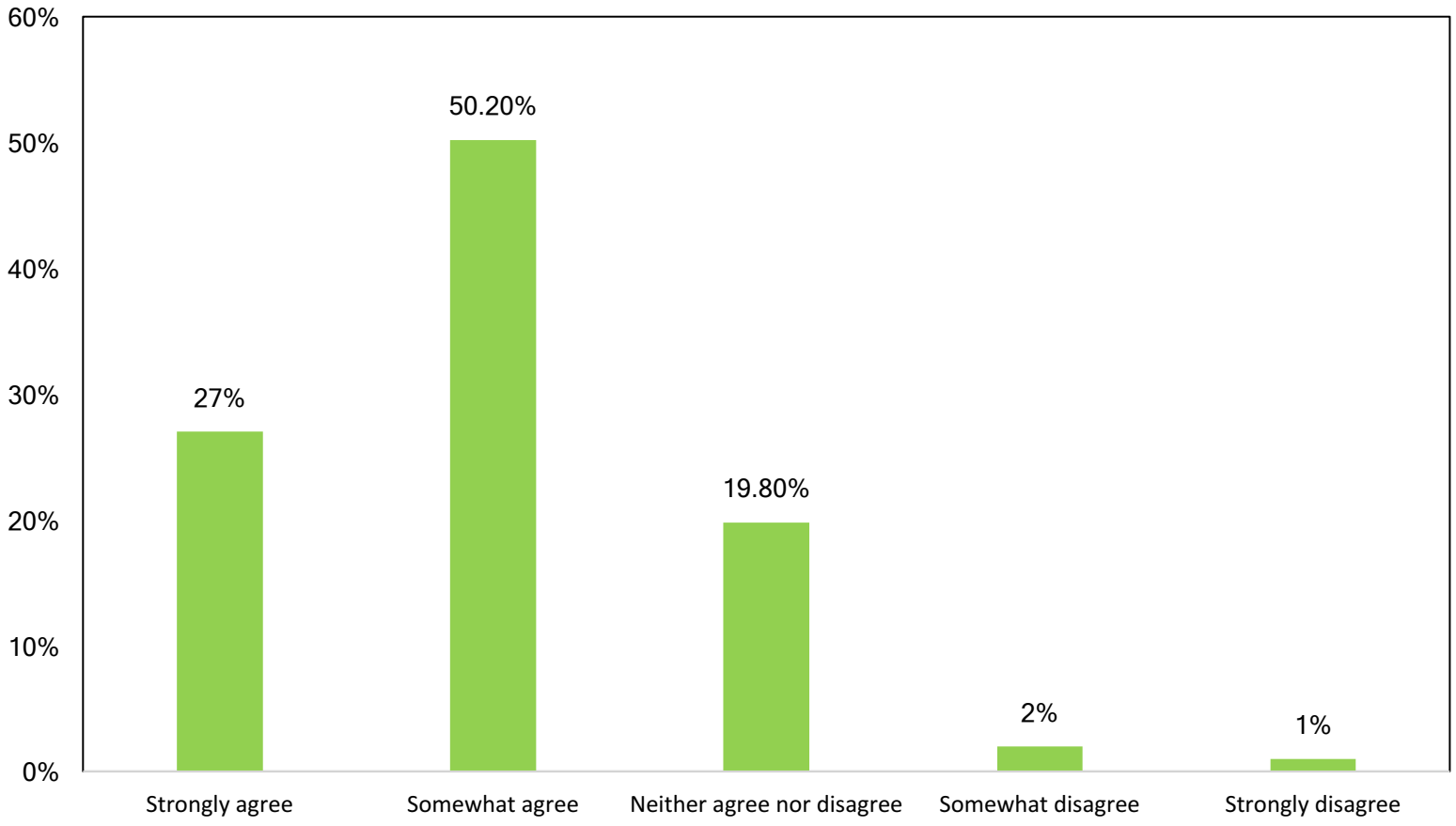
If it were legal, would you be more inclined to recommend 'hacking back' to recover decryption keys after a ransomware attack, or paying the perpetrator(s) to get back online?



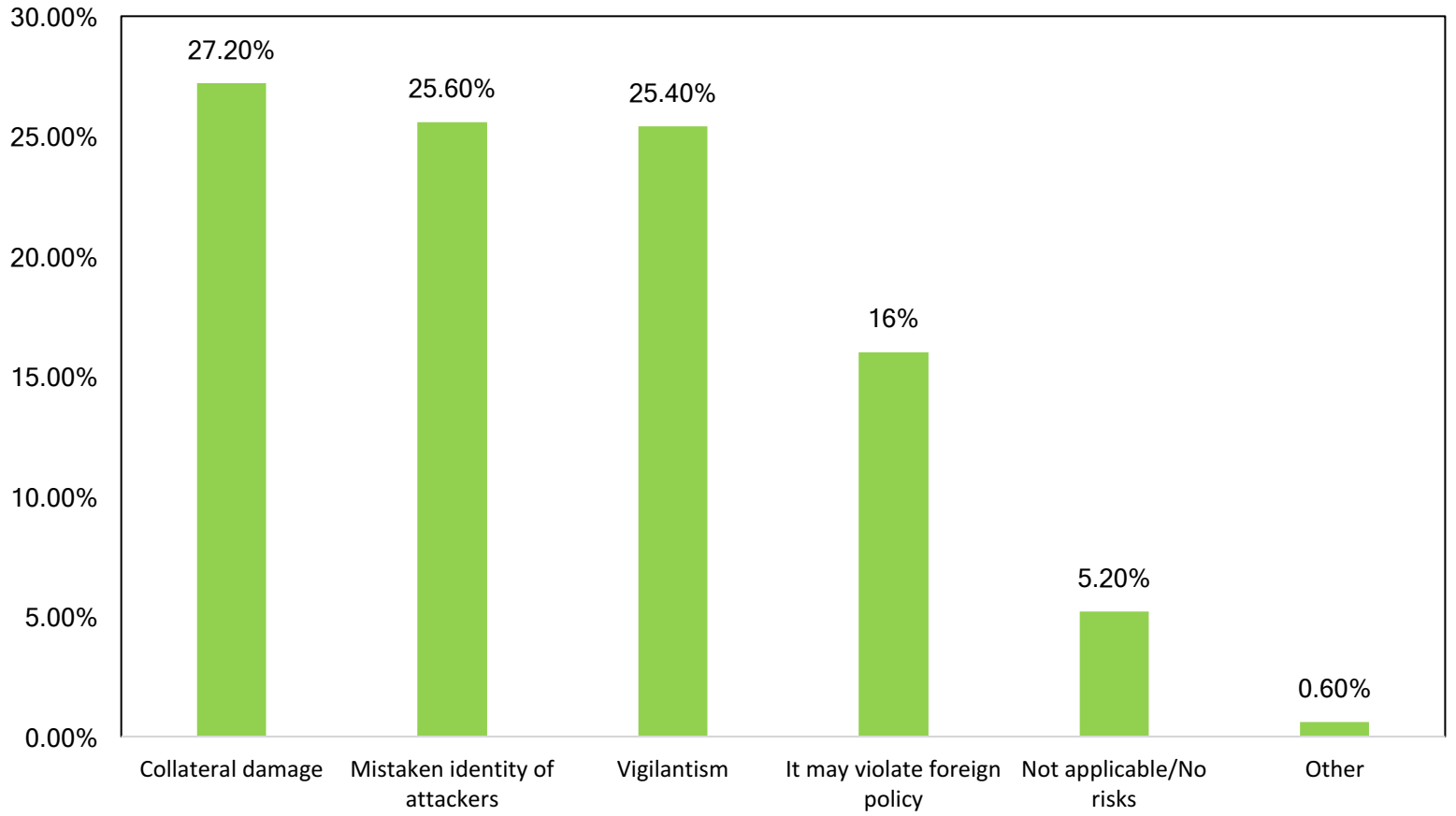
How far do you agree or disagree with the following statement? ‘Offensive Security’ could lead to a new generation of methods and tools to retaliate against cyber attacks



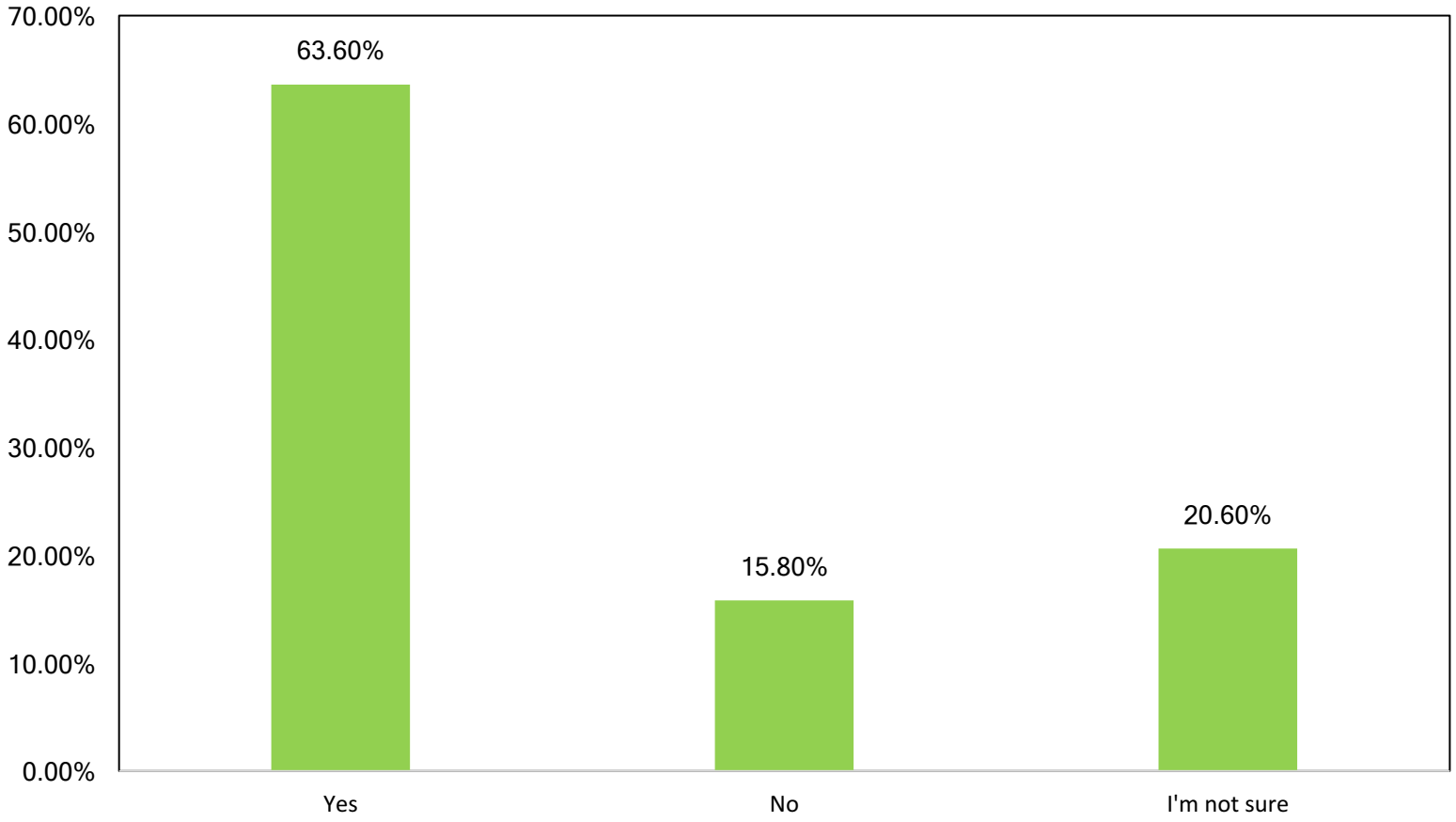
How far do you agree or disagree with the following statement? Deception technology is one of the first steps towards ‘offensive security’



If available, what do you see as the most worrying risk of ‘hacking back’?

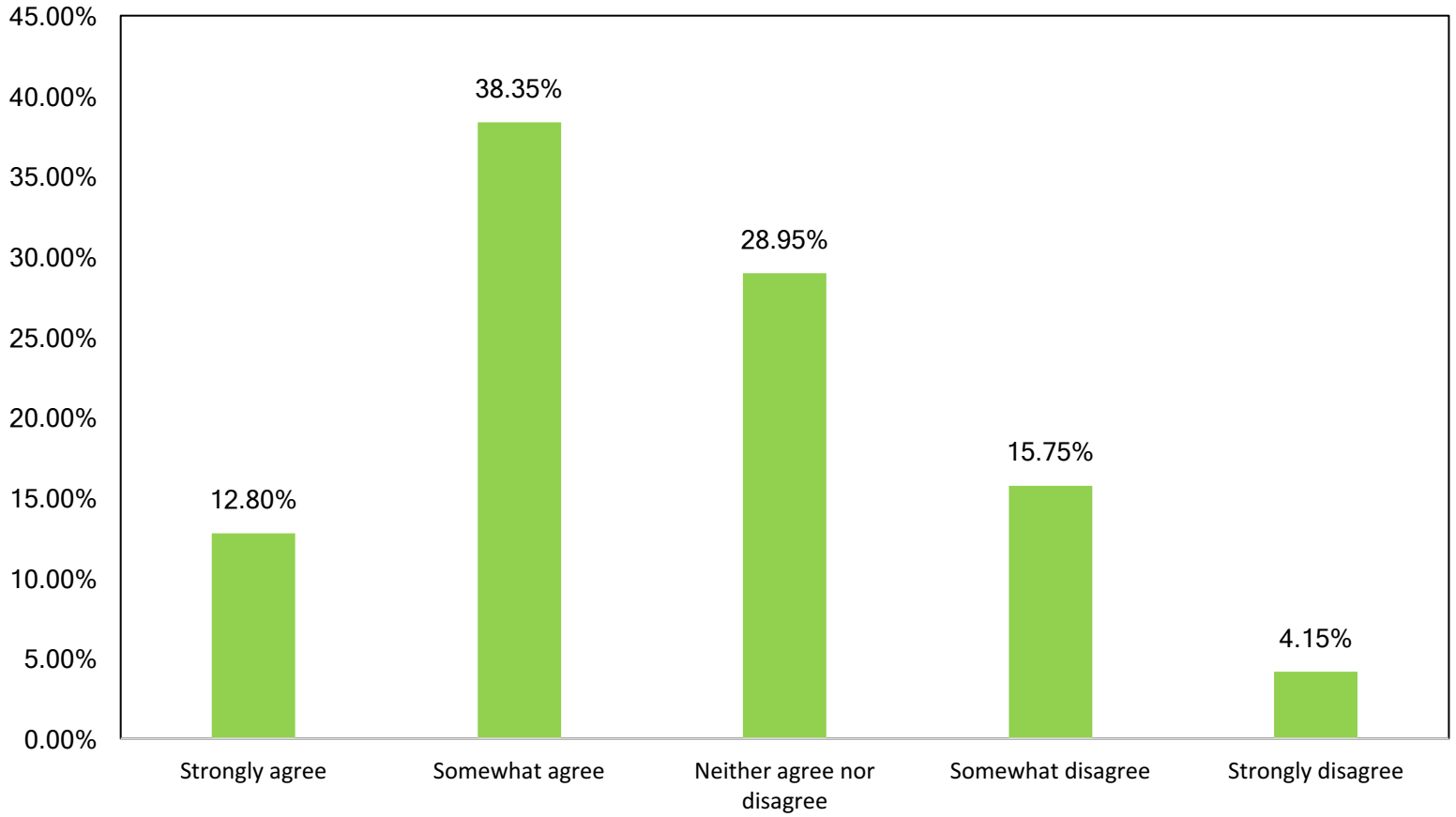


If companies were financially liable for any damage caused to innocent computers as part of 'offensive security,' do you think that your company would be less likely to enforce it?

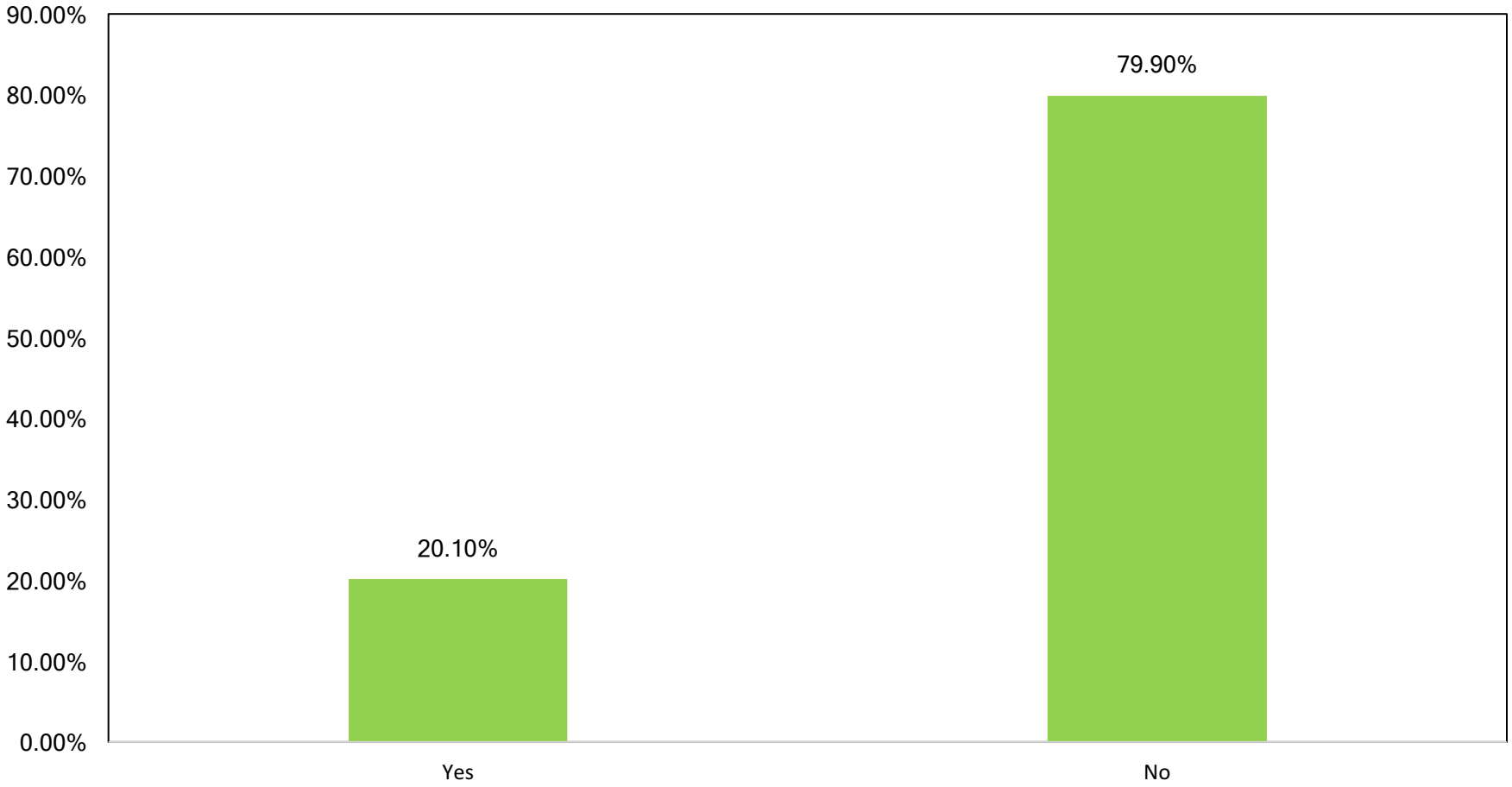


Consumer survey: The results

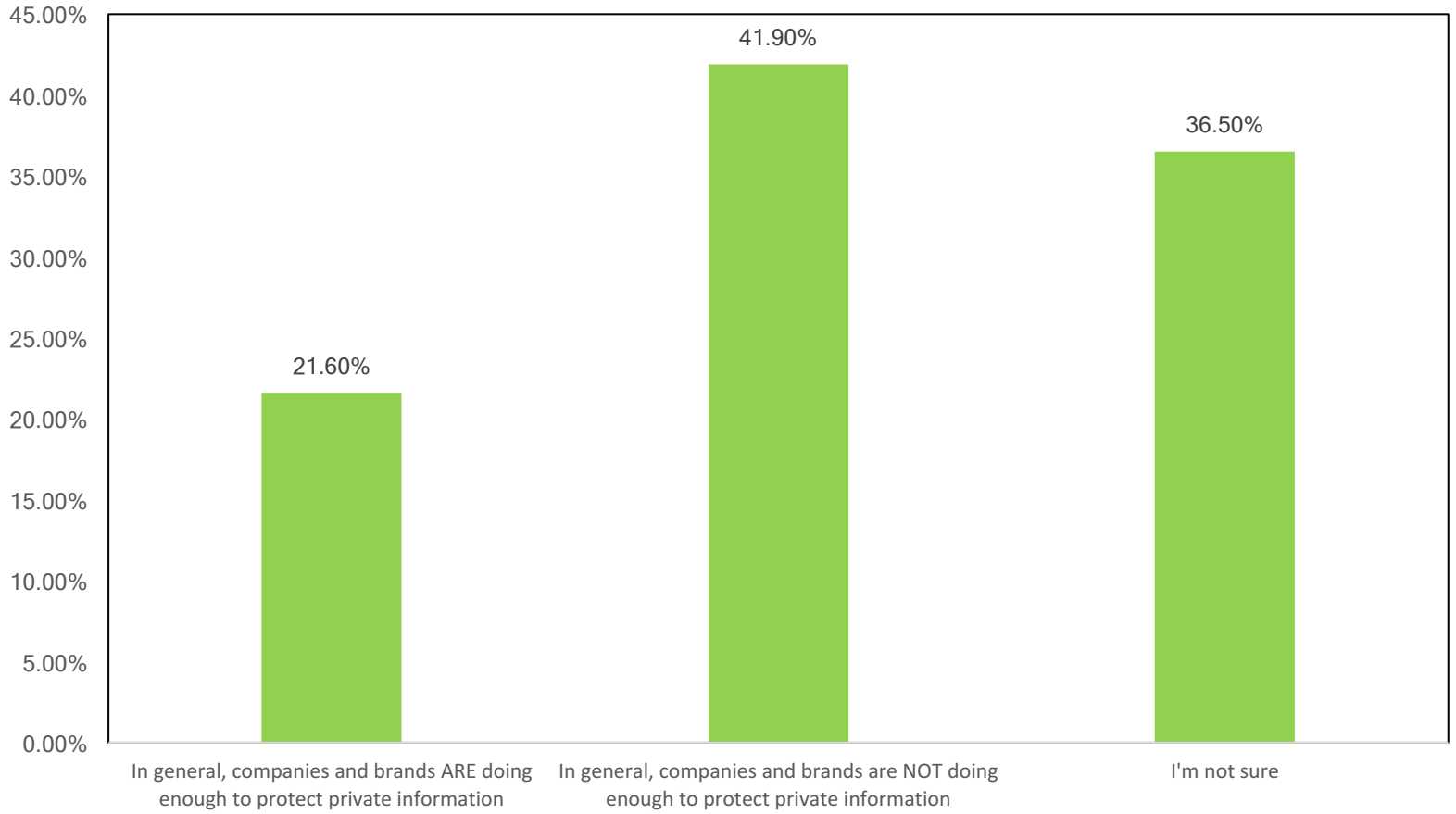
How far do you agree or disagree with the following statement? It has become inevitable that my personal data (i.e. email address, credit card details, usernames, passwords, date of birth, etc.) will be compromised by hackers at some point



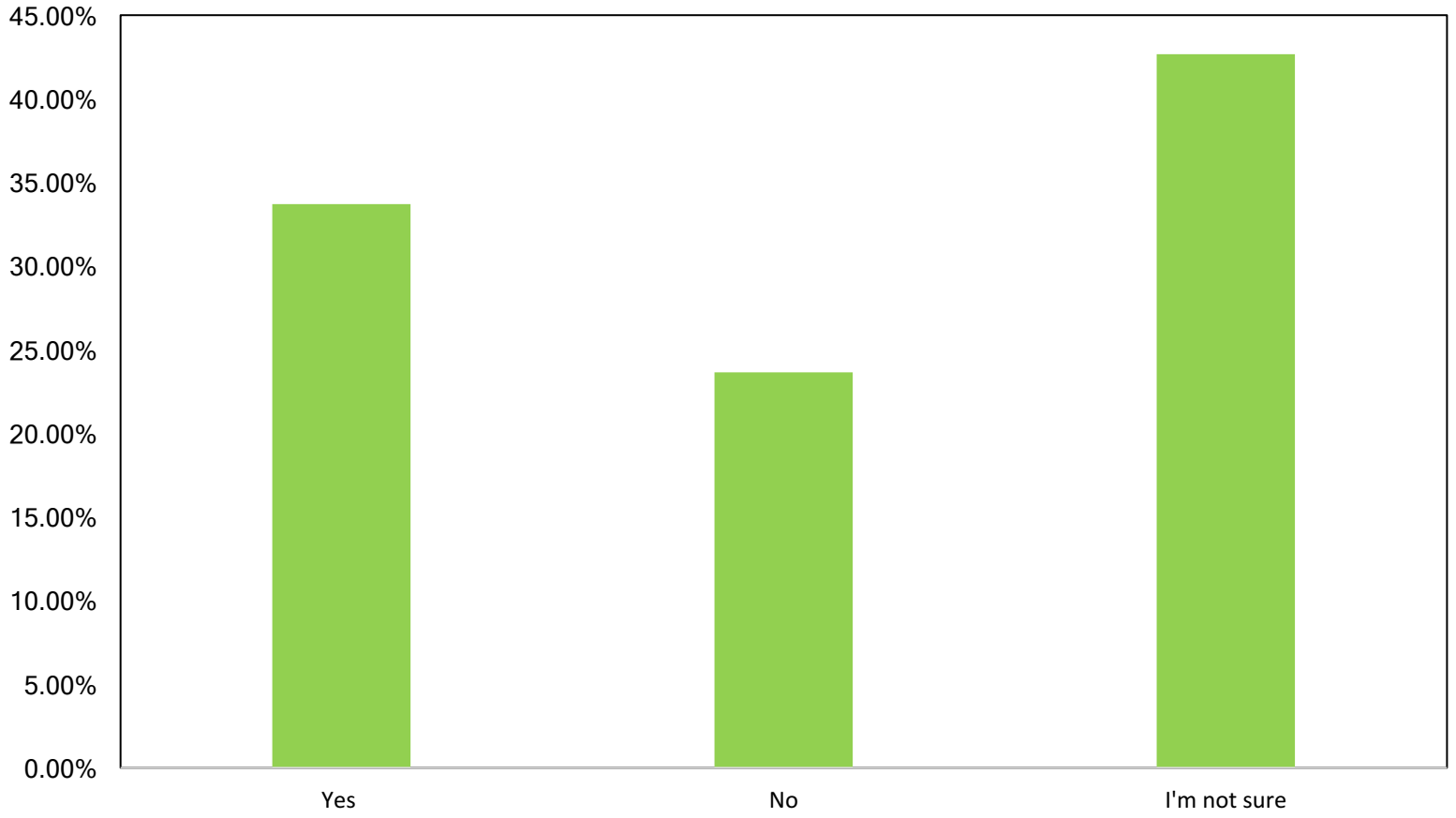
Have you ever stopped buying goods or services from a company or brand as a direct result of them experiencing a data breach?



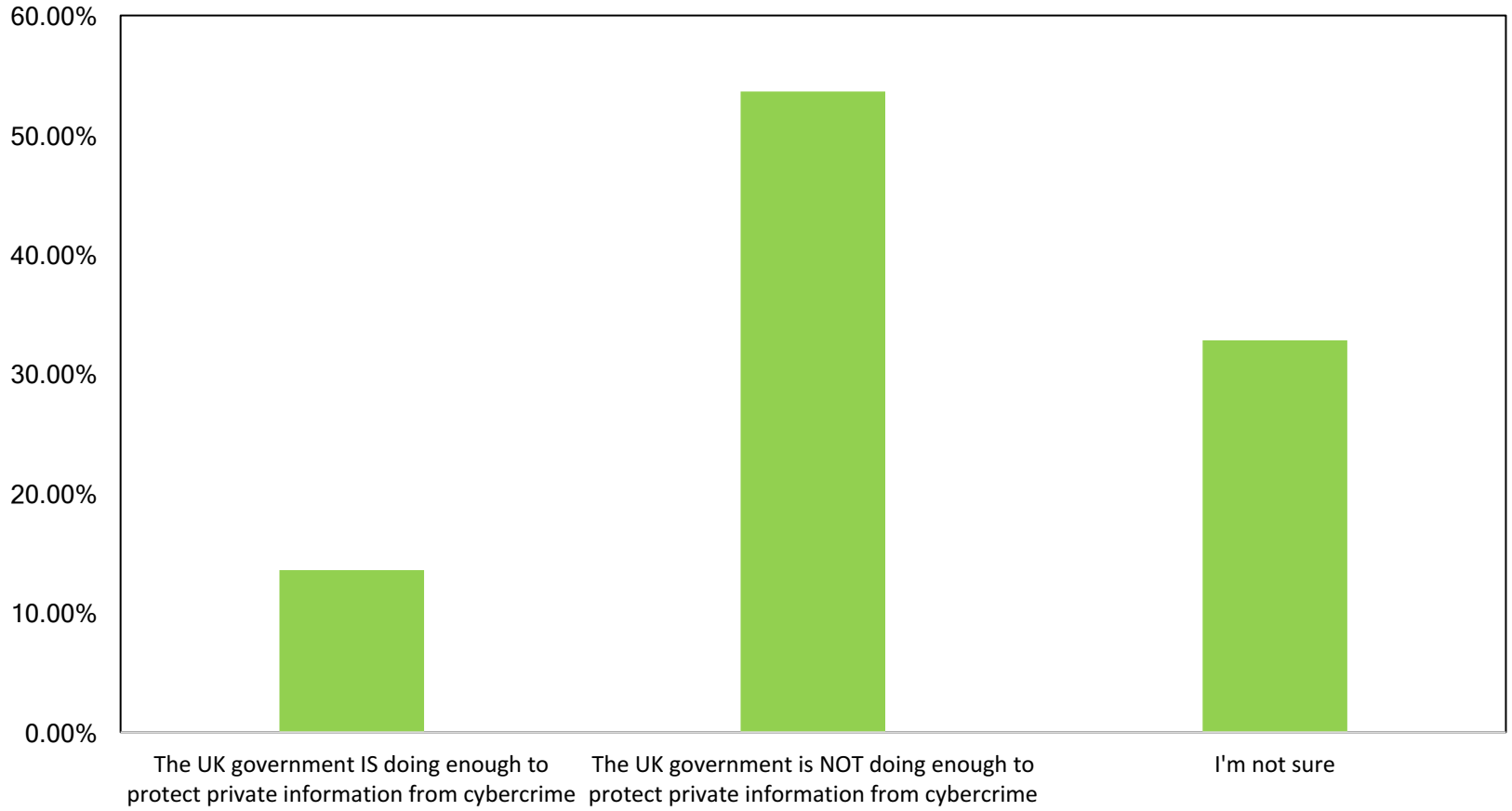
In regards to what is being done by companies and brands to prevent data breaches and protect private information from cyber security threats, which one of the following best describes your opinion?



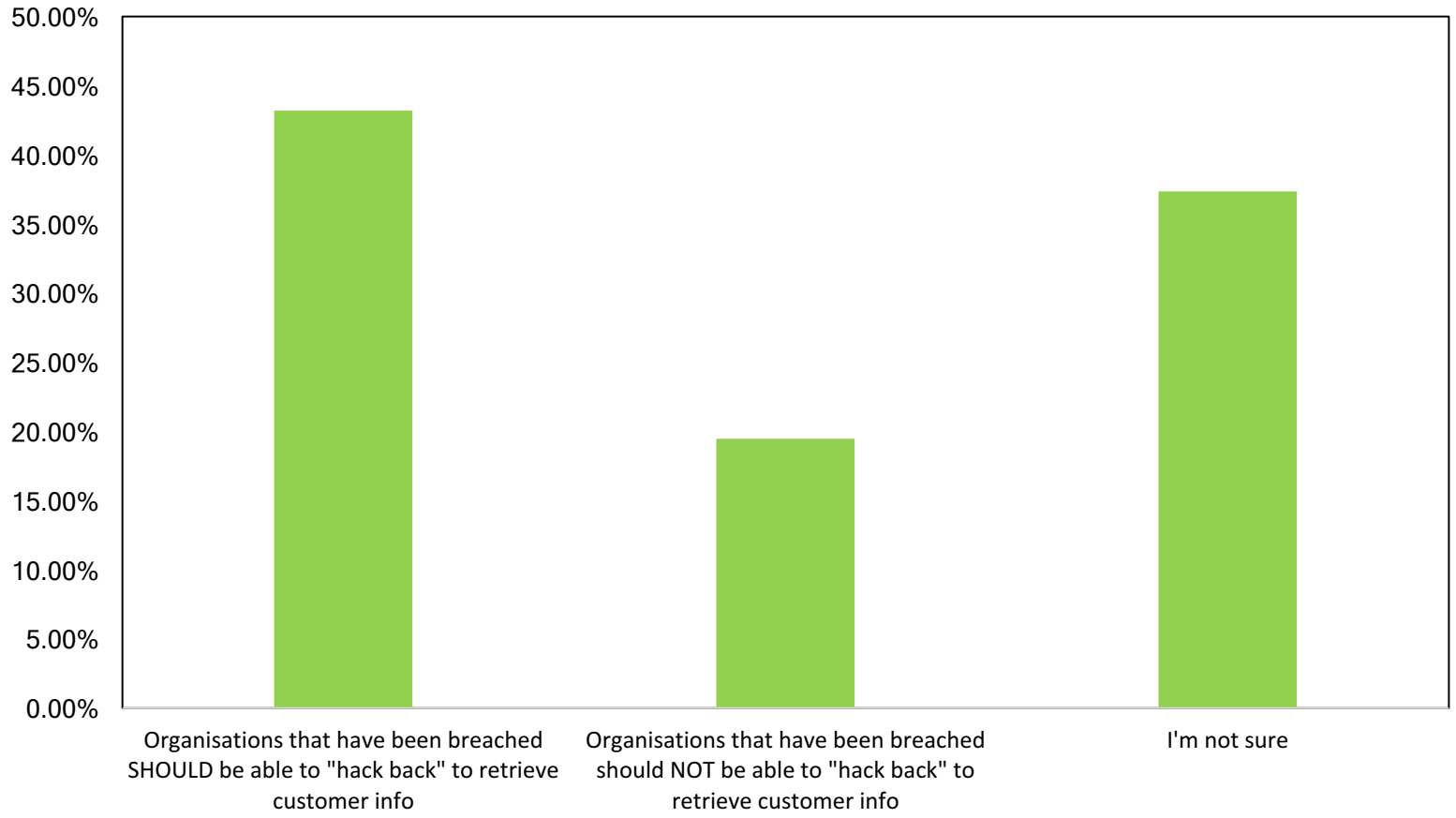
Do you think that you would pay more to use a supplier that has a strong commitment to preventing data breaches and is vocal about the technology in place to prevent personal data loss, than to use one that did not?



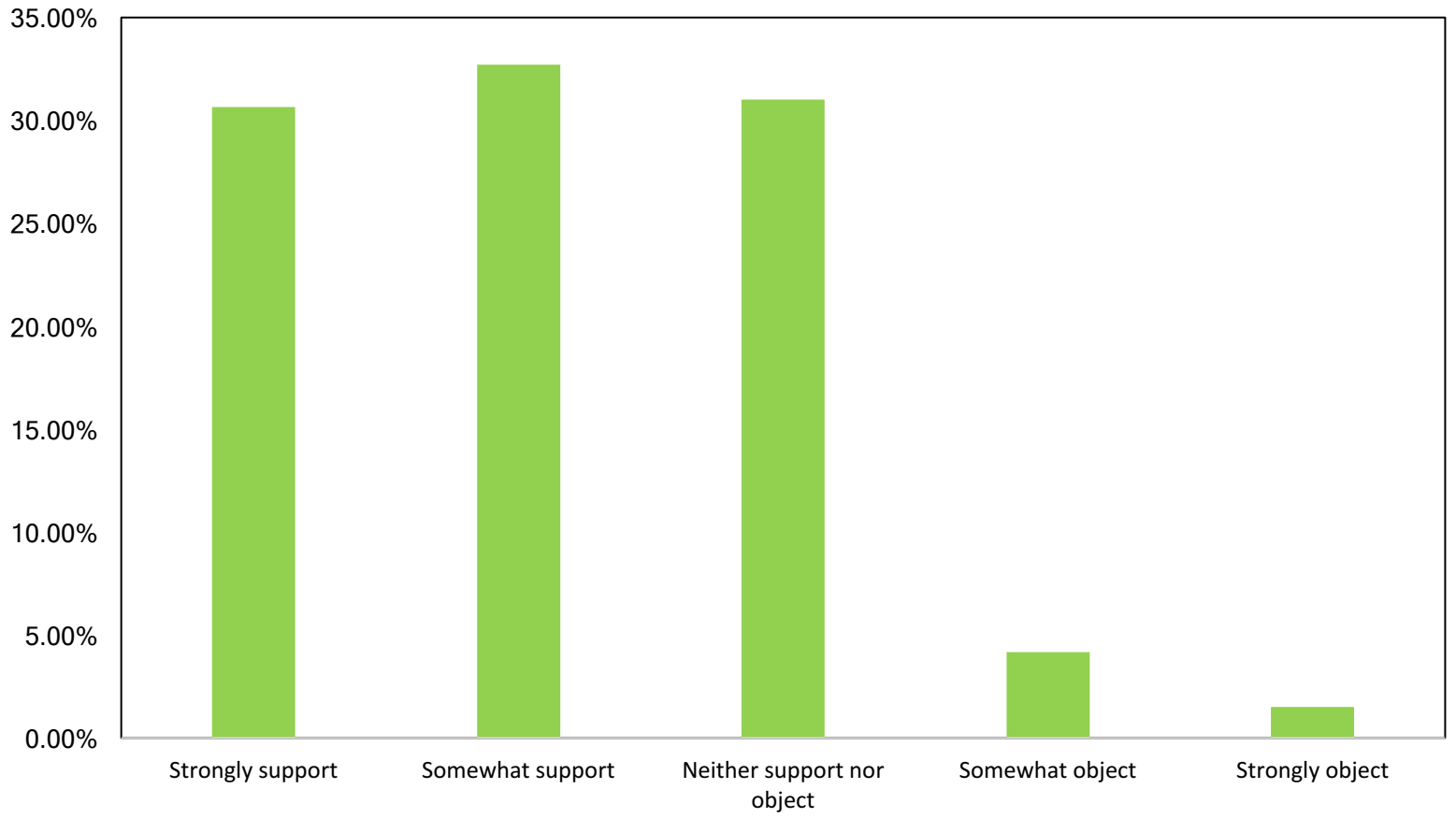
In regards to the UK government's strategy for protecting private information from cyber security threats, which of the following best describes your opinion?



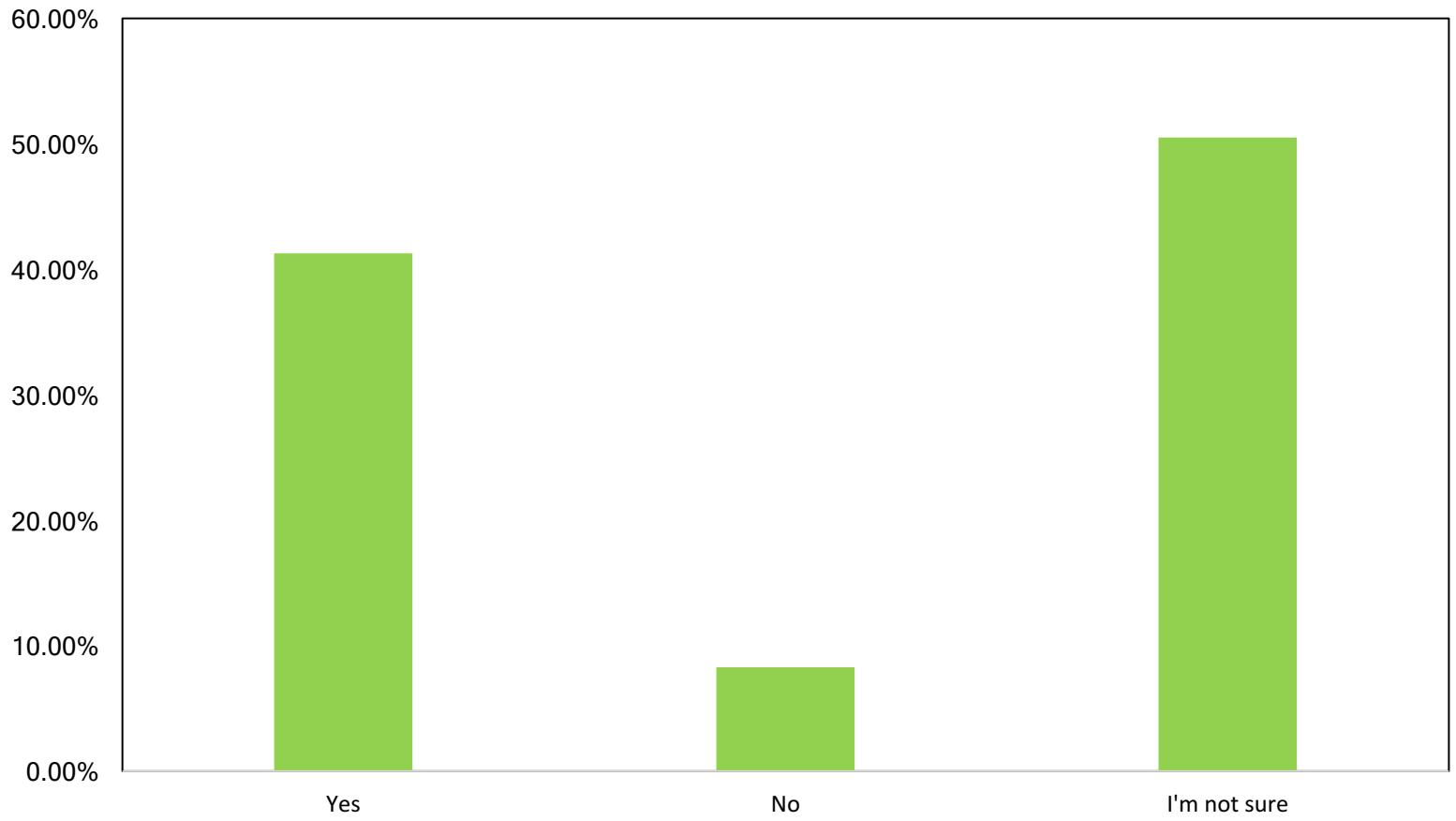
In regards to organisations who have suffered a cyber-attack and lost sensitive customer information, which of the following best describes your opinion?



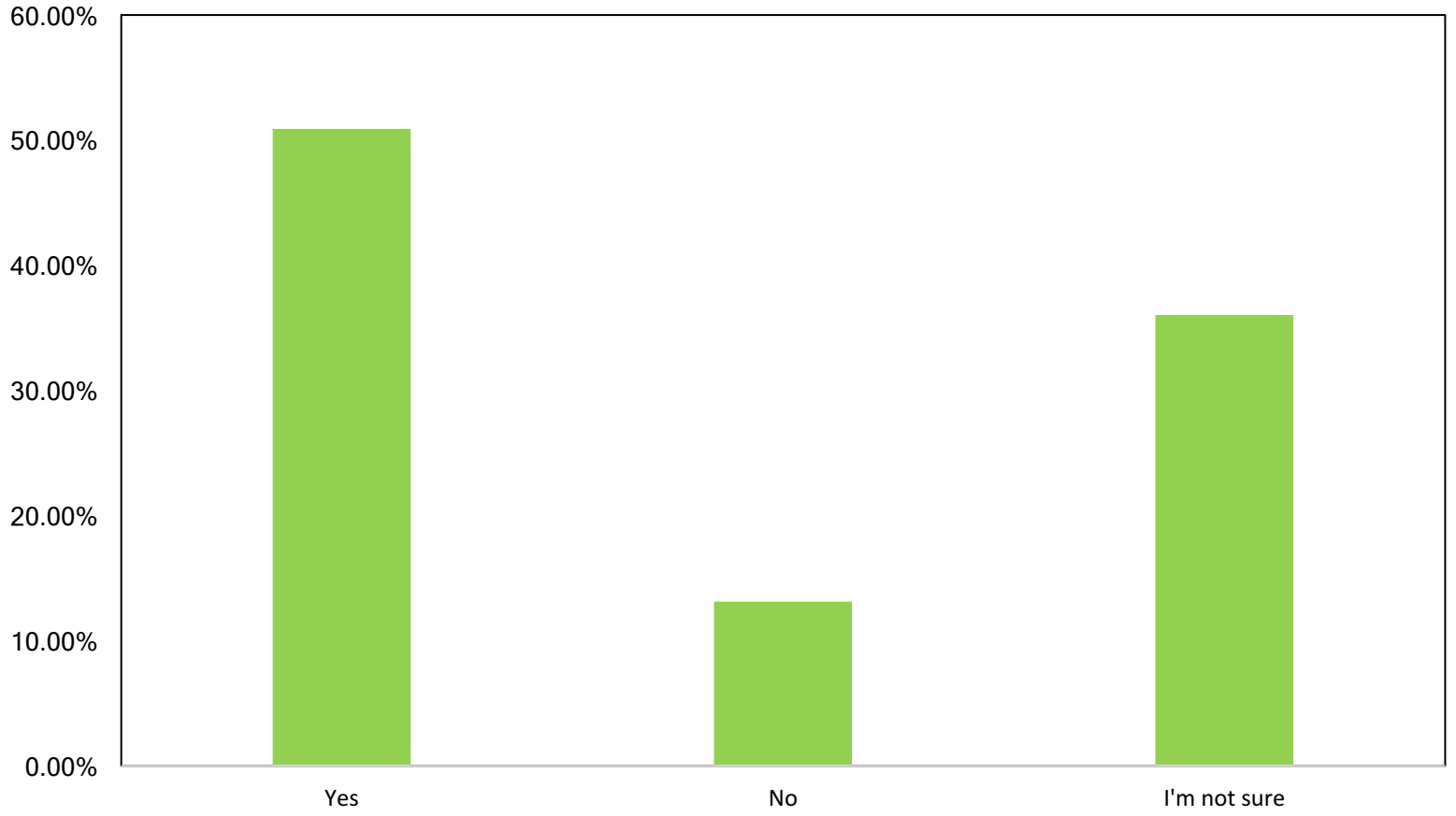
To what extent would you support or object to legislation that would allow security experts to ‘hack back’ your stolen information?



In general, do you think there are any risks with companies being able to 'hack-back' your stolen information?



Do you think that a parent should be able recover and destroy stolen ‘intimate’ pictures of their children that are being used by criminals to extort them?



About Fidelis Cybersecurity

Fidelis is the only integrated, automated network and endpoint detection and response platform. The company's Elevate™ platform improves the efficiency and effectiveness of security operations teams by condensing alert data into actionable threat summaries and then automating response and investigation. With automatic validation, investigation and prevention of attacks, Fidelis is engineered for visibility, designed for response and trusted by the most important brands in the world.

For more information: www.fidelissecurity.com

Fidelis™ Cybersecurity