PULSE Bravura Security

THE RISING INSIDER THREAT:
Hackers Have Approached 65% of Executives or Their Employees To Assist in Ransomware Attacks

Ransomware attacks regularly generated prominent news coverage in 2021, and they are continuing to grow in frequency, complexity and sophistication. Yet, there is another facet of ransomware attacks that has not received the same attention in the media: insider threats.

Since our last survey conducted in November, there has been a 17% increase in the number of employees and executives who have been approached by hackers to assist in ransomware attacks. To combat this rising threat, businesses must take a proactive offensive approach to cybersecurity or face financial and reputational damage.

To gain a better understanding of the different types of ransomware threats, Pulse and Bravura Security surveyed 100 IT and security executives on how hackers are approaching employees, how ransomware is impacting an organization's cybersecurity approach, and how prepared businesses really are to combat these attacks.

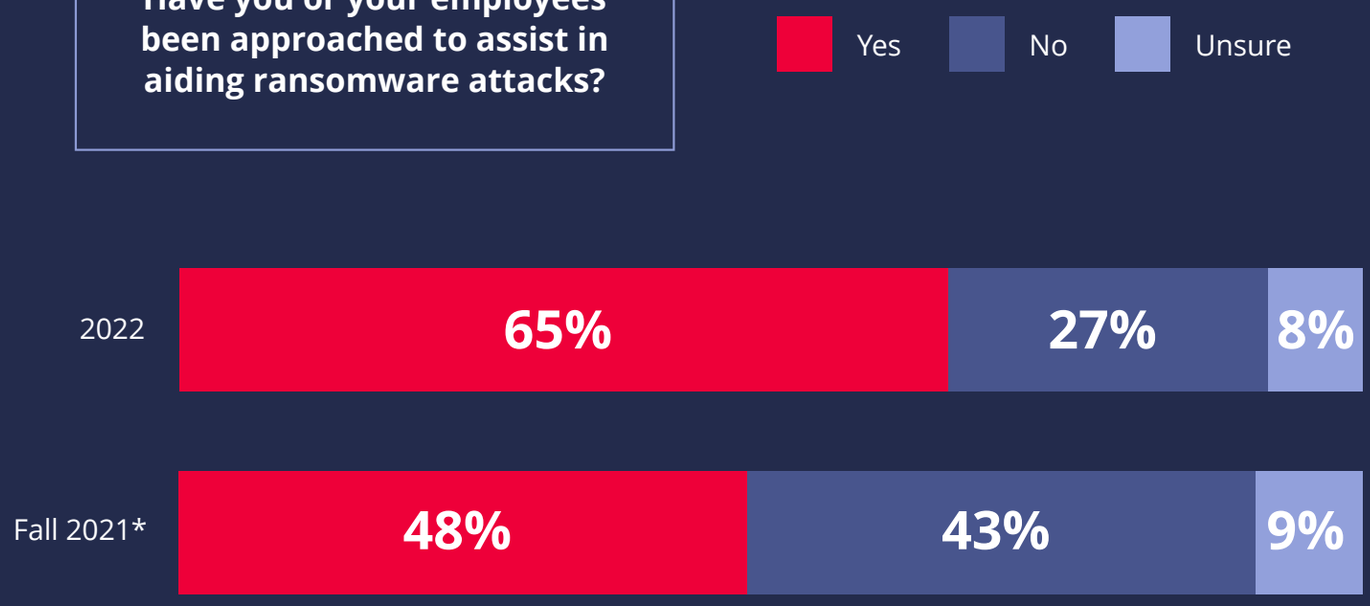
Data collected from December 7, 2021 - January 4, 2022

Respondents: 100 IT and security executives

EMPLOYEES AND LEADERS HAVE INCREASINGLY BEEN APPROACHED TO ASSIST IN RANSOMWARE ATTACKS—PRIMARILY THROUGH EMAIL

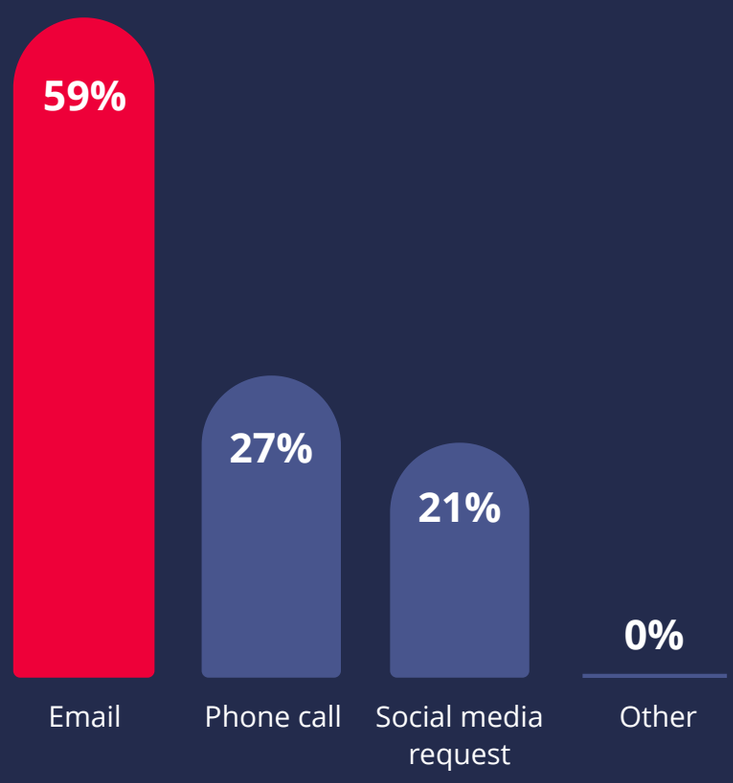
Over half (65%) of respondents say they or their employees have been approached to assist in aiding ransomware attacks. Interestingly, this is a 17% increase in comparison to a similar survey run in the Fall of 2021.

Have you or your employees been approached to assist in aiding ransomware attacks?



*Fall 2021 question: Have you or your employees been approached directly to assist in planning ransomware attacks?

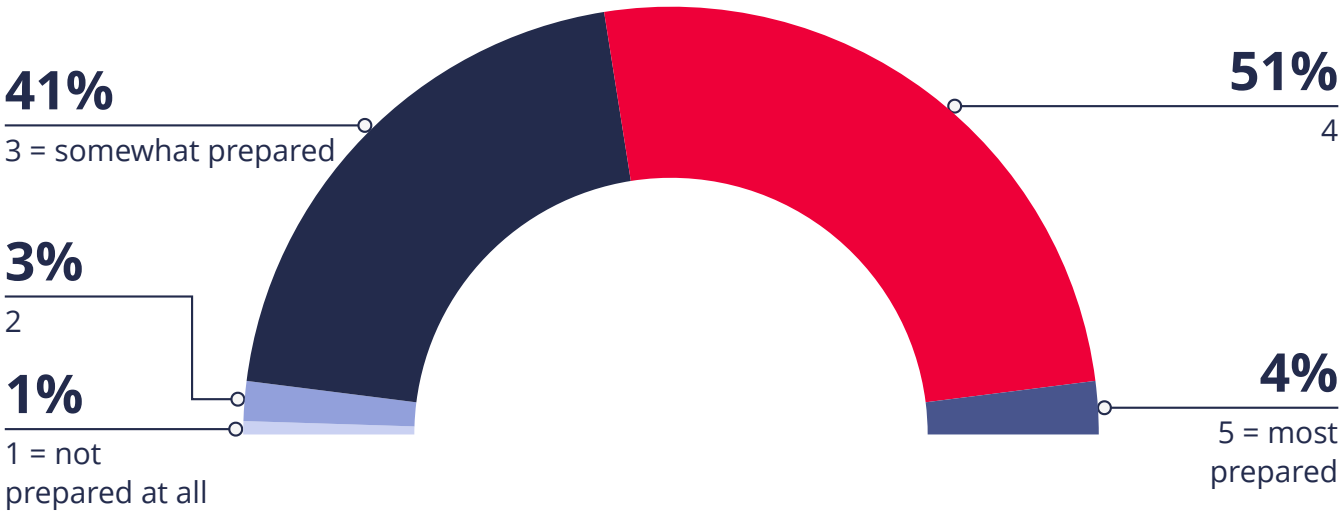
How were you/your employees contacted by ransomware attackers?



ALTHOUGH MANY CONSIDER THEMSELVES PREPARED TO DEFEND AGAINST RANSOMWARE, RELIANCE ON PERIMETER DEFENSE MAY PRESENT A WEAK LINK

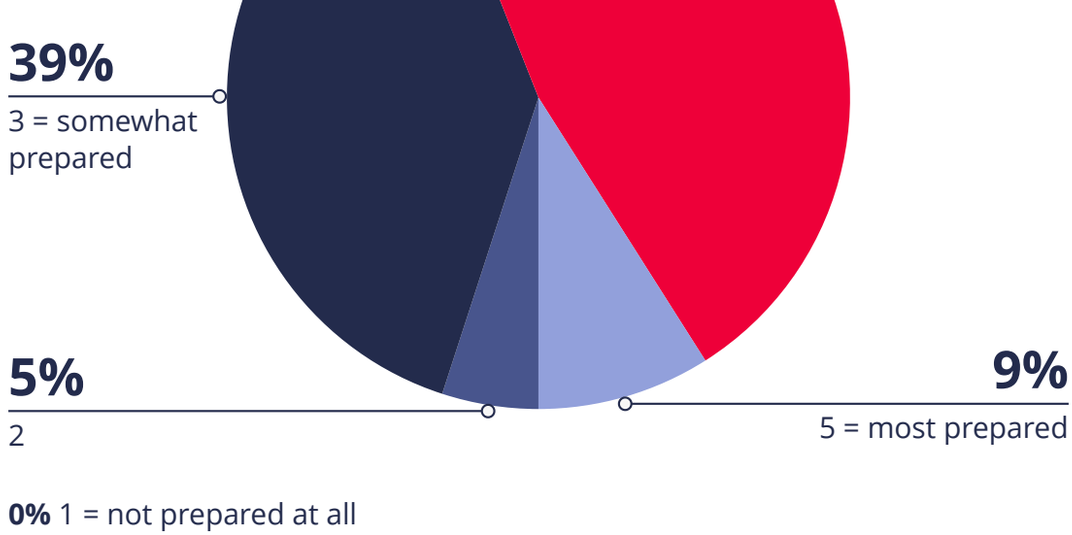
Roughly half (51%) of executives feel moderately prepared to prevent a ransomware attack, with 4% saying they feel most prepared.

On a scale of 1-5 with 5 being the most prepared, how prepared do you feel your organization is to prevent a ransomware attack?



Similarly, in the event that a hacker breaches their system, 56% of leaders say their organization is moderately or most prepared to reduce the damage or stop the attack.

Once a hacker breaches your system, how prepared is your organization to reduce the damage or stop the attack? Scale of 1-5 with 5 being most prepared.



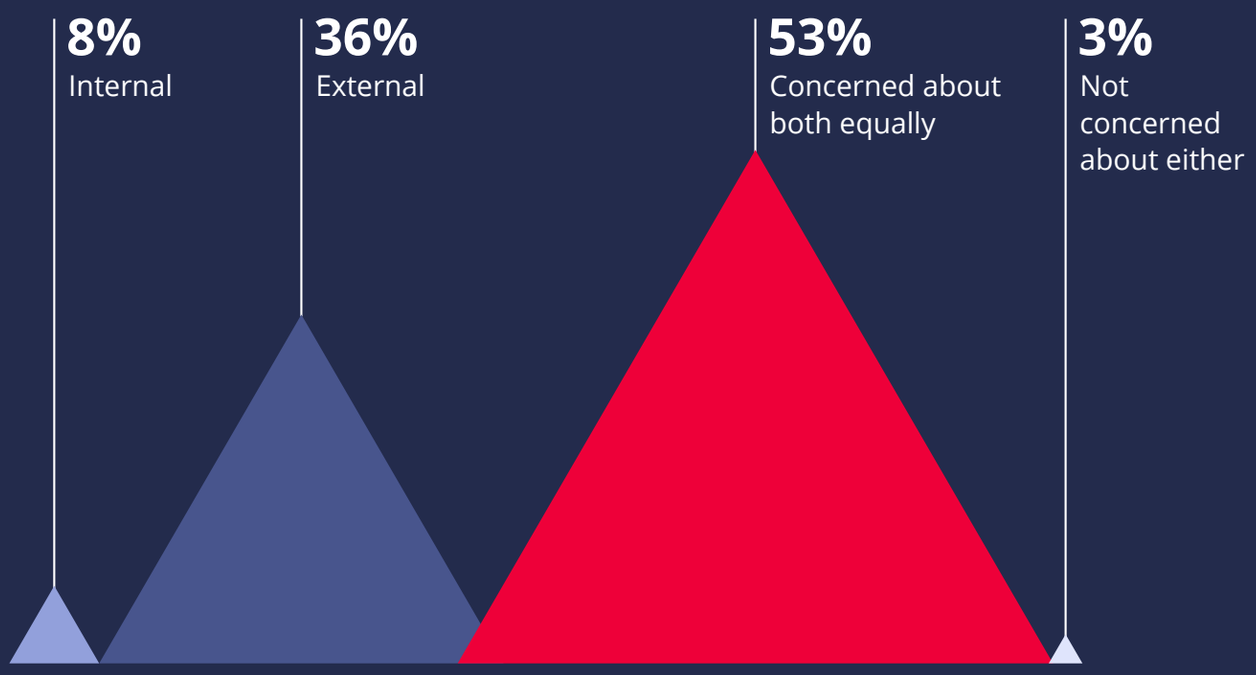
However, most decision-makers stated that they mostly rely on perimeter defense (45%), with 6% exclusively using perimeter defense.

On a scale of 1-5, how much does your organization rely on perimeter defense?

CYBERSECURITY MEASURES MUST ACCOUNT FOR INTERNAL AND EXTERNAL THREATS

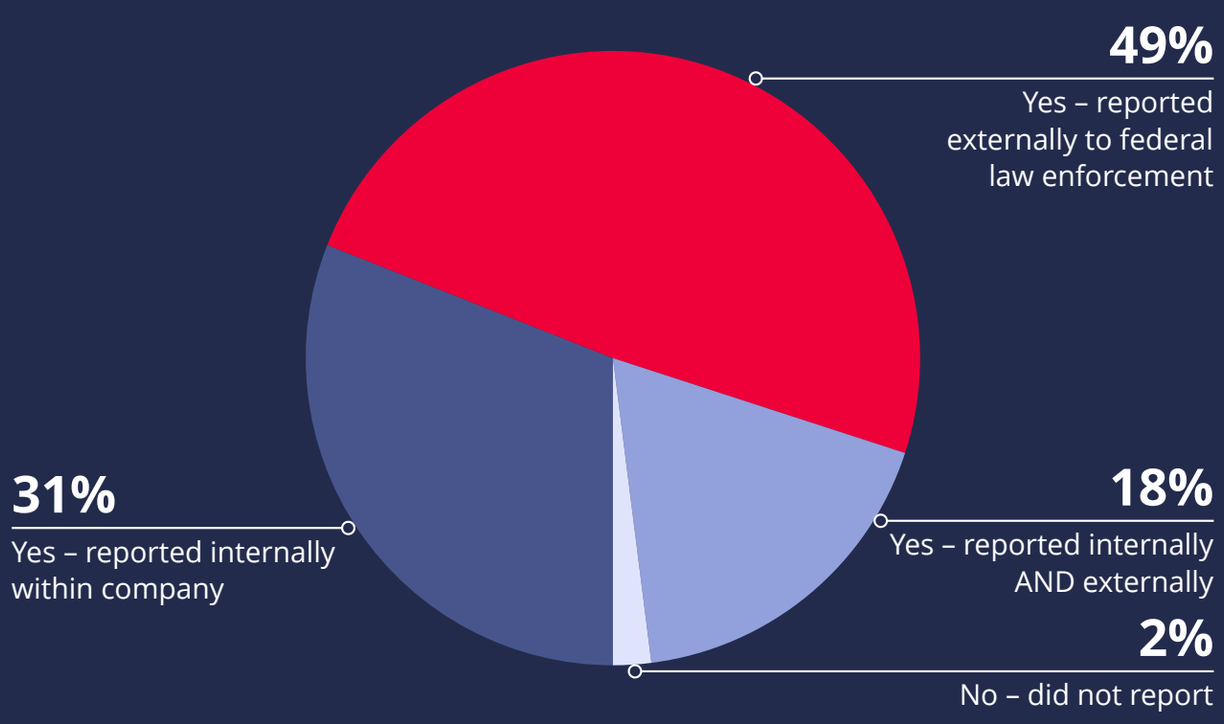
While 36% are more concerned about external threats than internal ones, more than half (53%) are equally concerned about both.

Are you more concerned about internal or external cybersecurity threats?



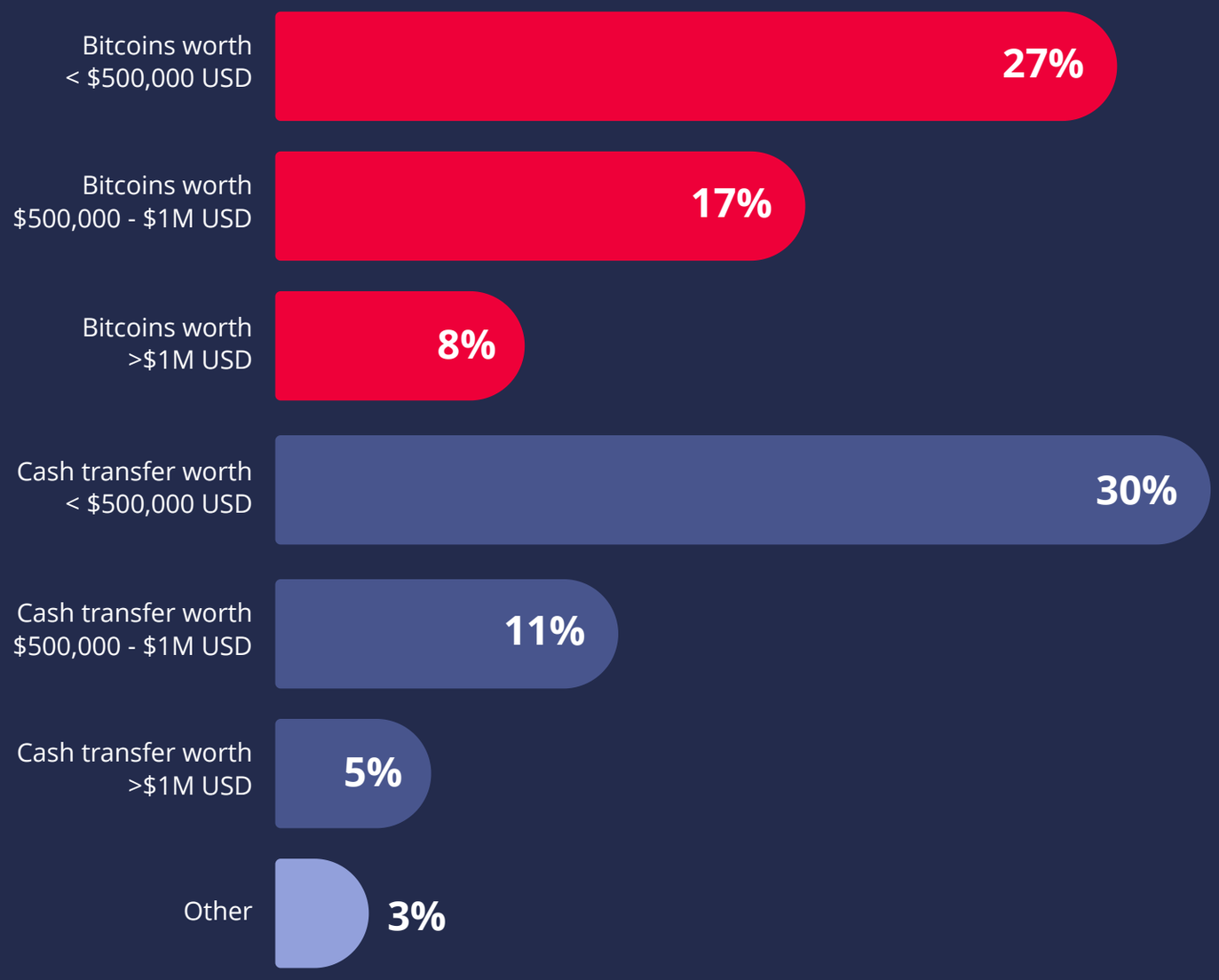
Of those who were approached to assist in a ransomware attack (n = 65), 49% reported the incident to federal law enforcement with only 18% who reported both internally and externally.

Did you/your employees report the incident?



Overall, 57% of respondents reported that they or their employees were offered cash or Bitcoins worth less than $500,000 USD.

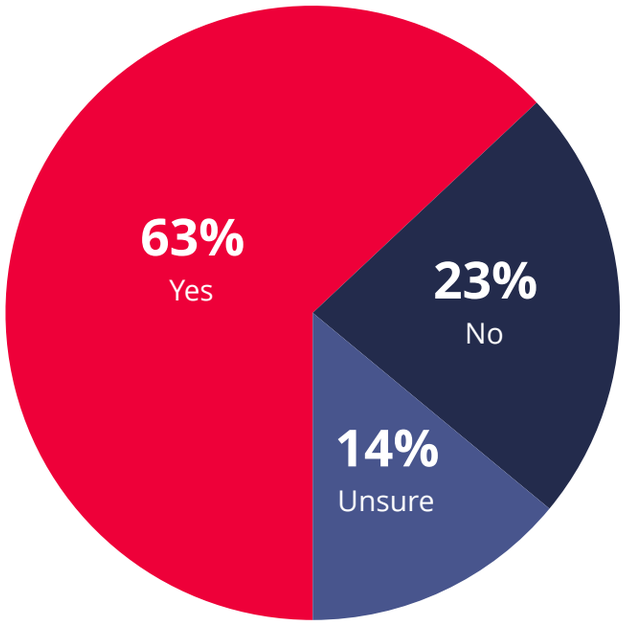
What were you/your employees offered in return for helping with the ransomware attack?



EXECUTIVES CONTINUE TO INVEST IN CYBERSECURITY MEASURES EVEN WHEN THEY HAVE INSURANCE COVERAGE FOR RANSOMWARE

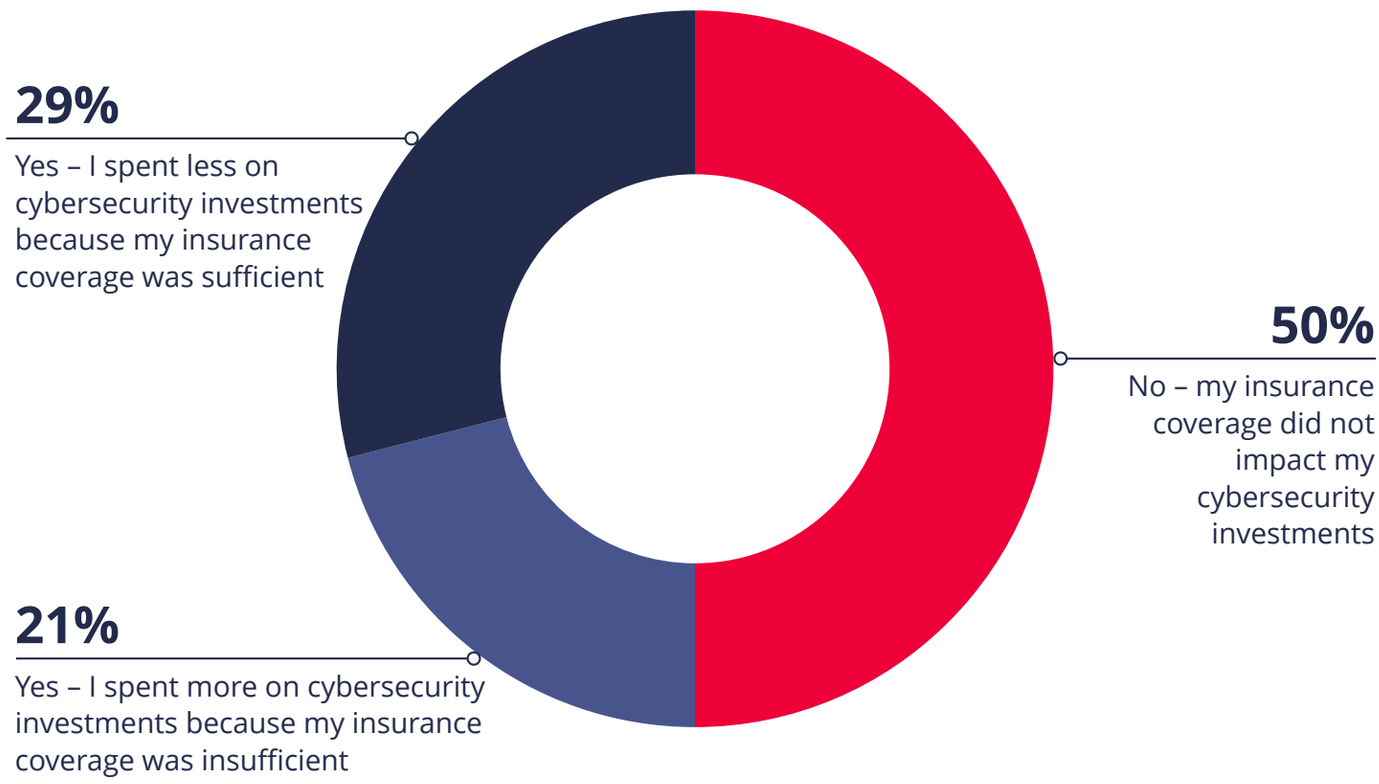
Most companies (63%) have an insurance policy that covers ransomware attacks.

Do you have an insurance policy that covers ransomware attacks?



50% note that their insurance policy did not impact their cybersecurity investments.

Did your insurance policy influence your cybersecurity investments?



Still, most (66%) have added or plan to add new security measures to curb ransomware attacks.

Have you added new security measures specifically to curb ransomware attacks?

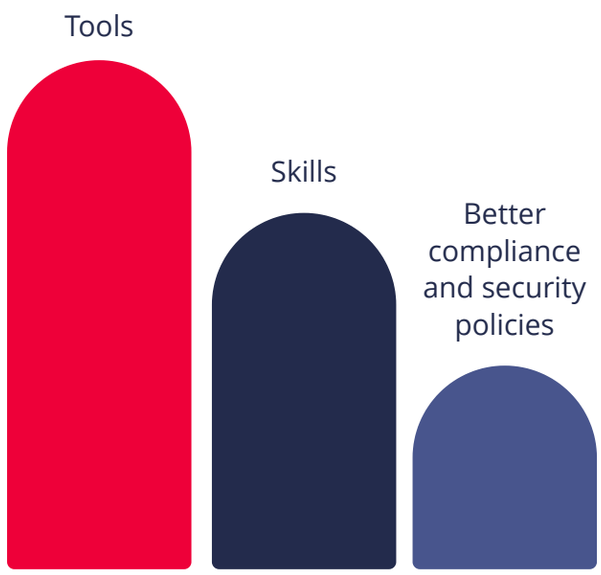
44%	22%	31%	3%
Yes	No, but I'm planning to	No	Unsure

Three of the top recurring themes for new security features were tools, employee skills, and better compliance and security policies.

In a few words, please specify these new security features.

"We increased our employee training and also send false requests in critical areas if we have reports of disgruntled employees or low performance review results."

- Director, Finance, Banking & Insurance, 10,000+ sized company



RANSOMWARE ATTACKS ARE MAKING HEADLINES, BUT HOW MANY BUSINESSES HAVE BEEN HIT? WHAT ARE THEY DOING ONCE ATTACKED?

38% of respondents say their company has been a victim of a ransomware attack.

Has your company been a victim of a ransomware attack?

38% Yes

44% No

18% Unsure

Of those who said they had been approached to assist in a ransomware attack (n = 65), 49% ended up a victim of ransomware attack.

Has your company been a victim of a ransomware attack?

49% Yes

32% No

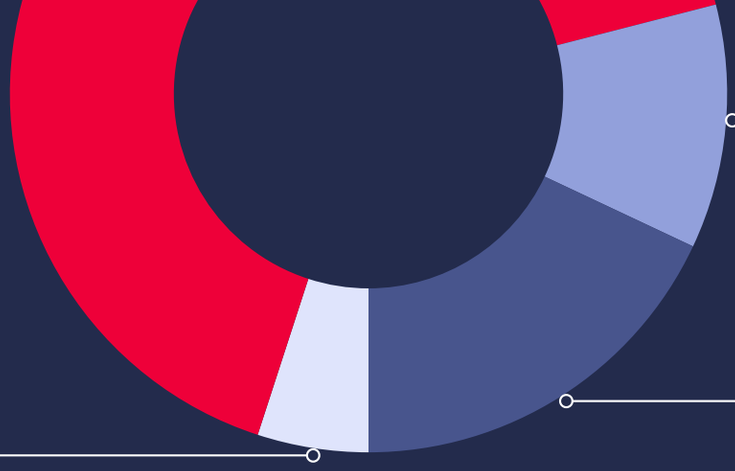
19% Unsure

Most consulted an external party before taking action and were advised not to pay ransom.

Once attacked, did you consult an external party (e.g. cybersecurity expert) before taking action?

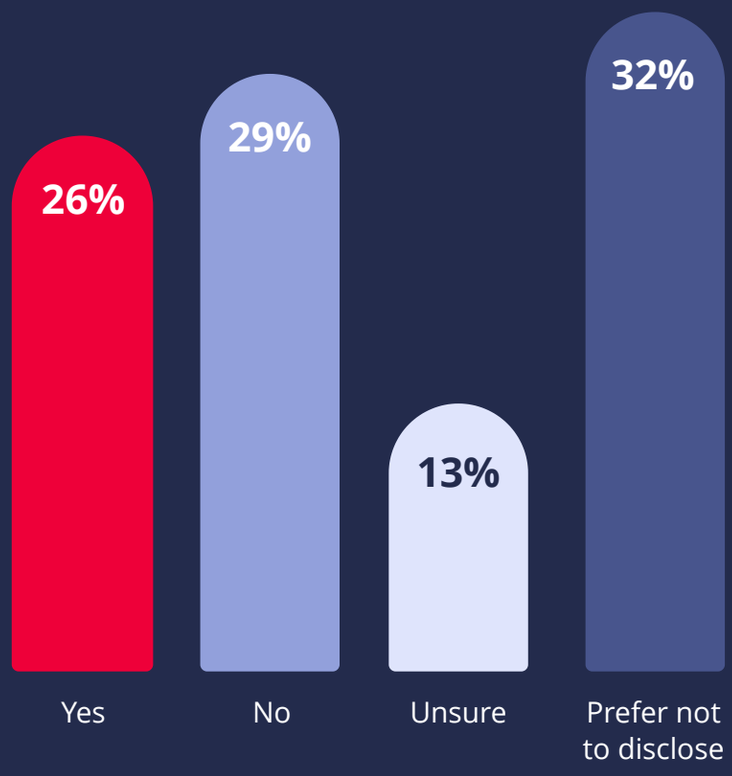
66%

Yes – was advised not to pay ransom



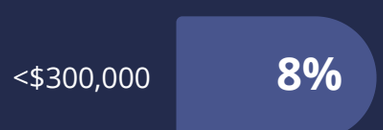
26% paid the ransom while 29% did not, although 32% chose not to disclose this information.

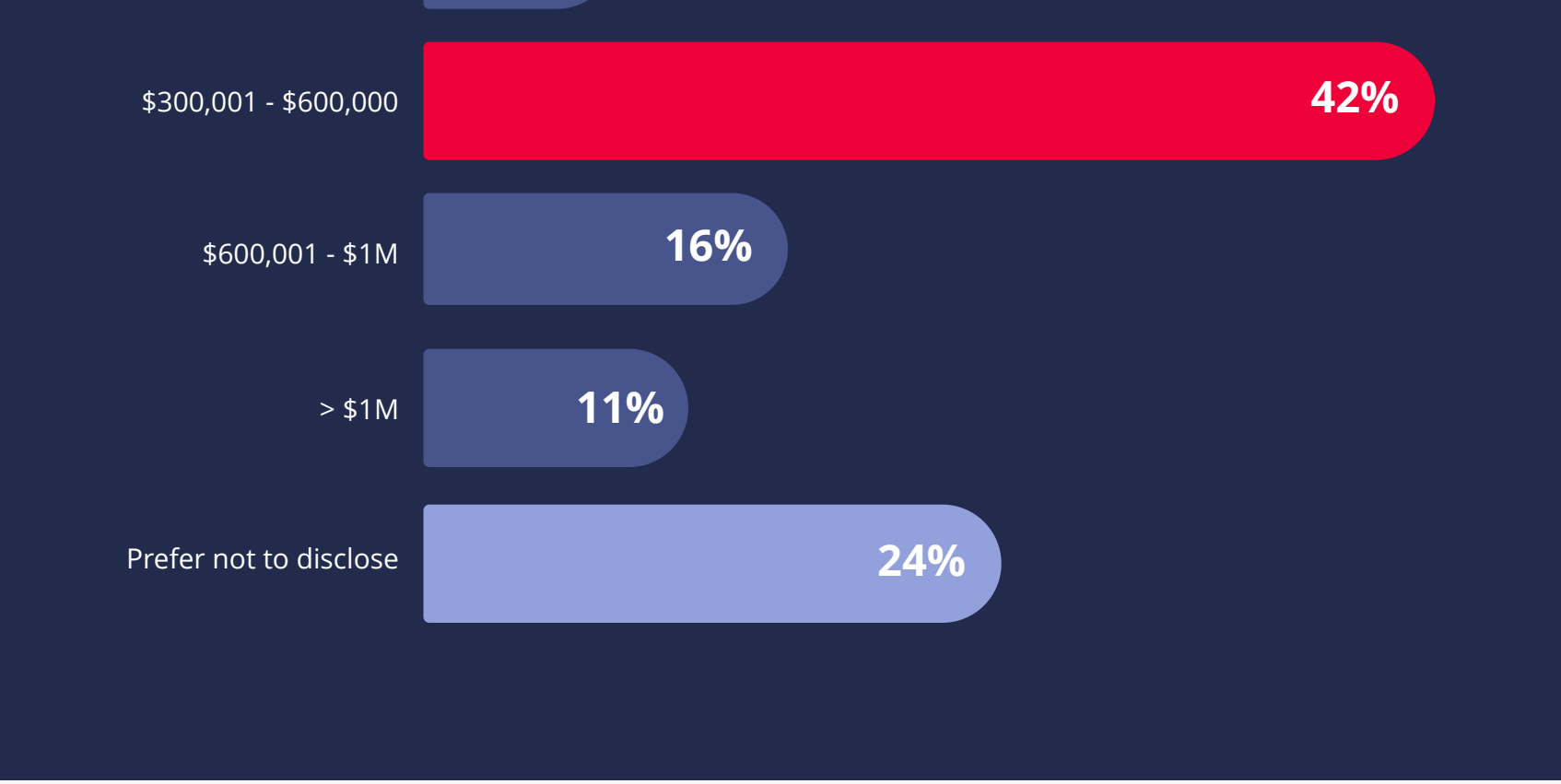
Did you pay the ransom?



Most ransomware requests were between $300,001 and $600,000.

How much was the ransom request for?





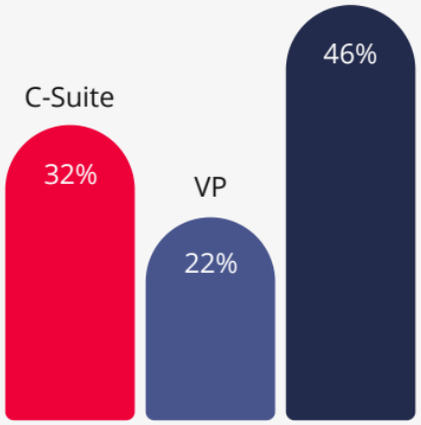
RESPONDENT BREAKDOWN

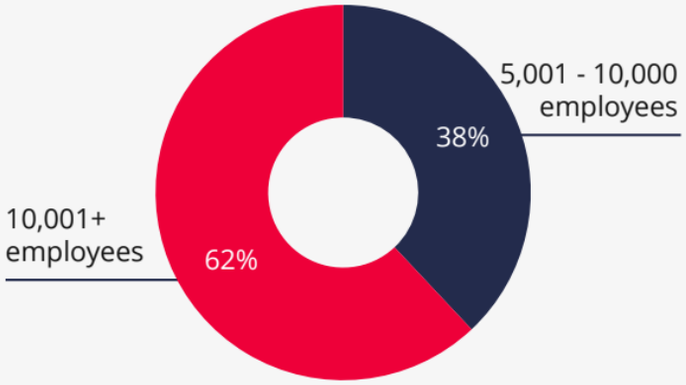
REGION

TITLE

Director

COMPANY SIZE





LEARN HOW AN IDENTITY-BASED SECURITY MODEL CAN PROTECT YOUR ORGANIZATION.

Bravura Security delivers cybersecurity protection with the industry's only single Identity, Privileged Access, Threat Detection, and Password Management platform and framework, the Bravura Security Fabric. Building on more than twenty years of deep domain experience, Bravura Security is an analyst-recognized leader and part of the global "One Bravura" portfolio.

bravurasecurity.com