Constella | PULSE

The Damaging Impact of Cybercrime on Executive Leadership

Ransomware attacks are on the rise, and no industry is immune. As the dust settles from some of the more recent newsworthy attacks, like the Colonial Pipeline, two things have become clear – ransomware is a present-day threat to companies of every size, and stolen employee credentials are fueling ransomware attacks.

Moreover, cyberattacks have increased in frequency during the COVID-19 pandemic, with threat actors utilizing more sophisticated tactics to gain access to PII, account or financial information of an employee. Executives and other key employees like IT personnel, HR and finance are attractive targets for cybercriminals as they have top-tier access to sensitive information and systems. When an employee's account is breached, it can trigger an earthquake for the entire enterprise, leading to severe financial and reputational damage.

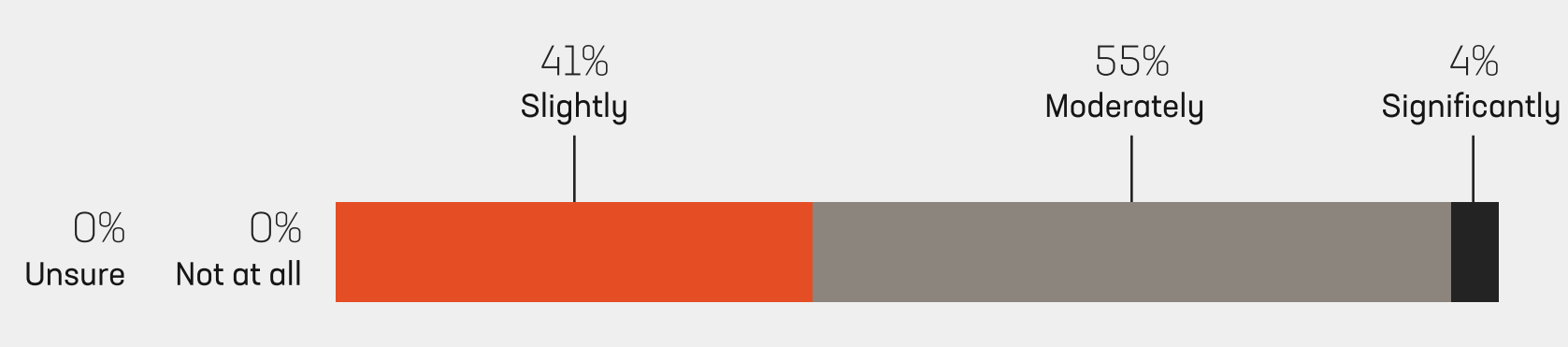
Pulse and Constella Intelligence surveyed 100 technology executives to understand the prevalence of cyberattacks like ransomware, on executive leadership and other key employees, the impact of cybercrime, and what measures leaders are taking to deal with these attacks.

Data collection: September 7 - October 18, 2021

Respondents: 100 technology executives

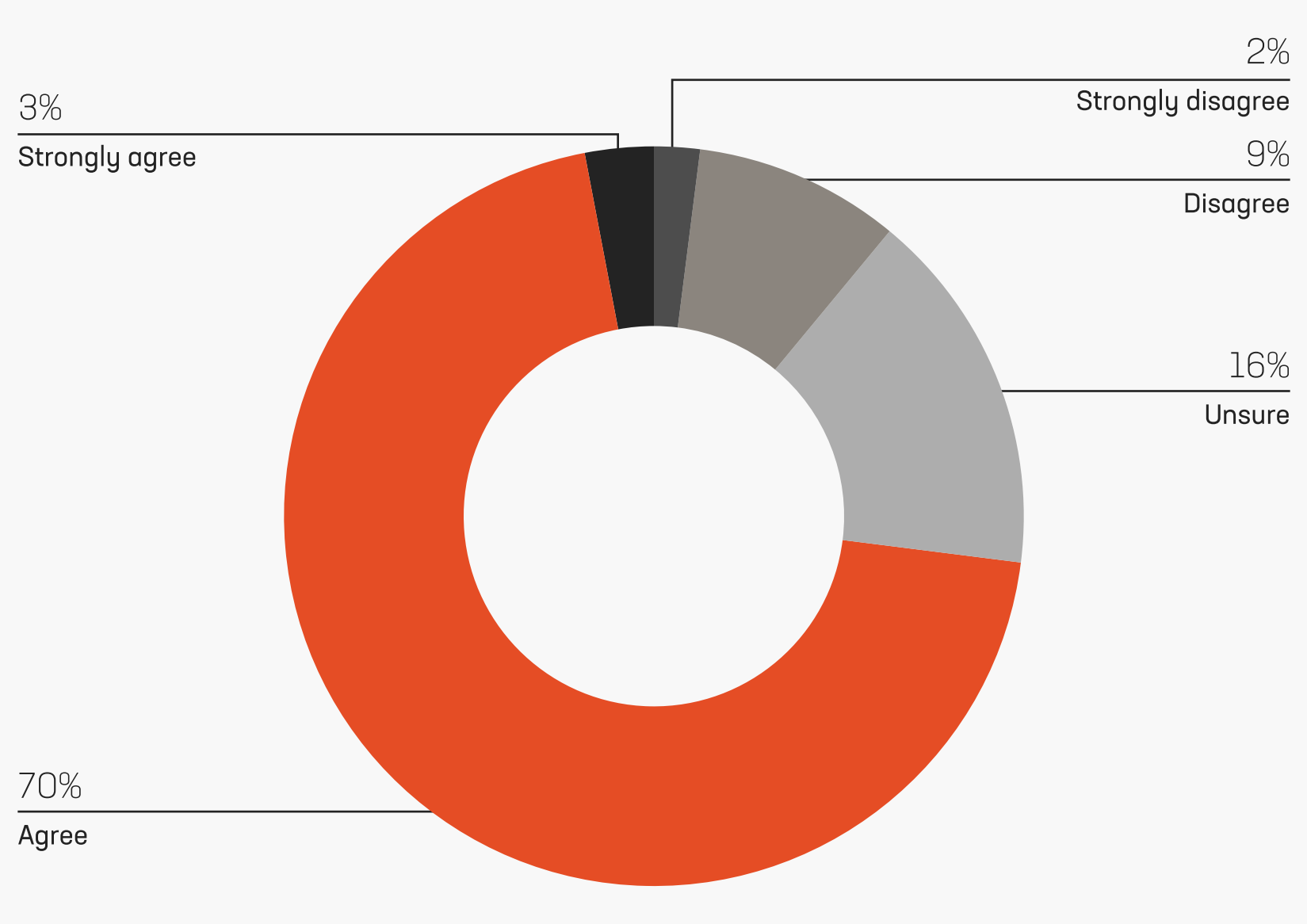
Remote work has led to increased attack surfaces and an uptick in vulnerability of executives to cyberattacks

DO YOU FEEL THAT YOUR ORGANIZATION FACES INCREASED CYBERSECURITY RISKS DUE TO REMOTE WORK?



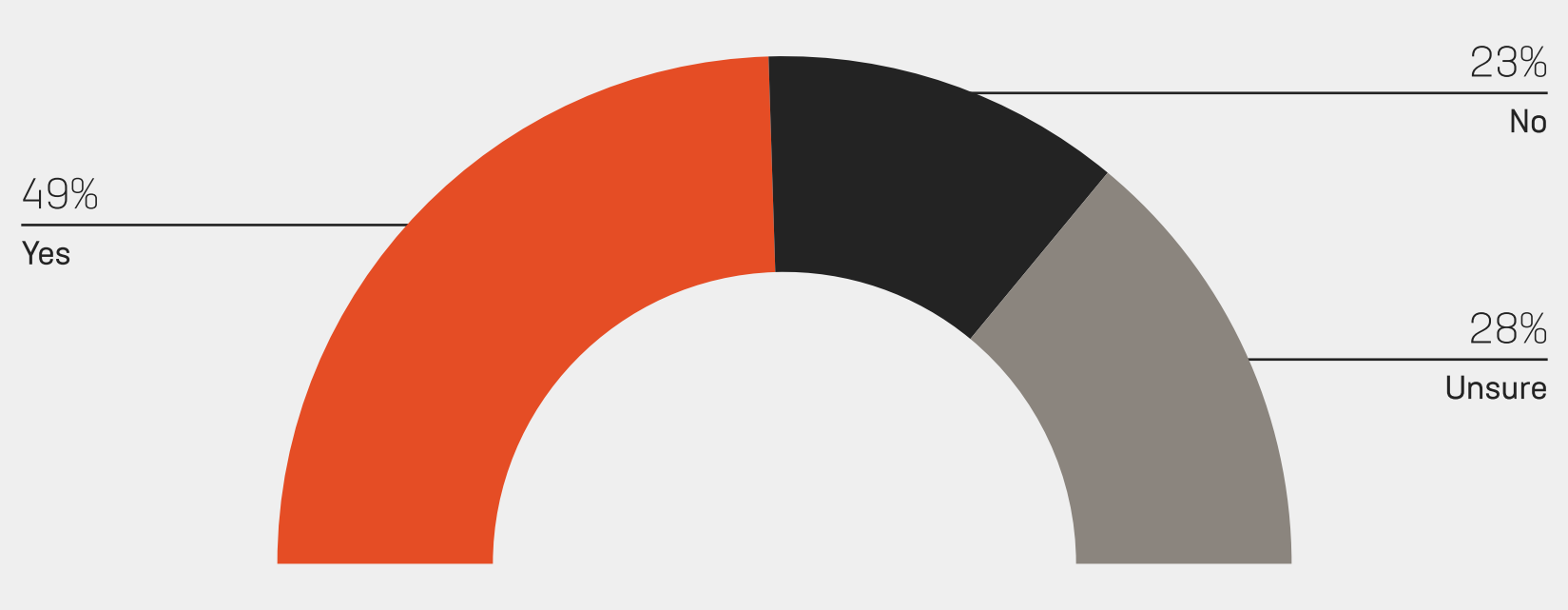
100% of executives, to some extent, feel that their organization faces increased cybersecurity risks due to remote work.

DO YOU AGREE WITH THE FOLLOWING? "EXECUTIVES AND PRIVILEGED IT PERSONNEL AT OUR ORGANIZATION ARE MORE VULNERABLE TO CYBERATTACKS WHEN THEY ARE WORKING REMOTELY."



73% of respondents agree that executives and privileged IT personnel at their organization are more vulnerable to cyberattacks when they are working remotely.

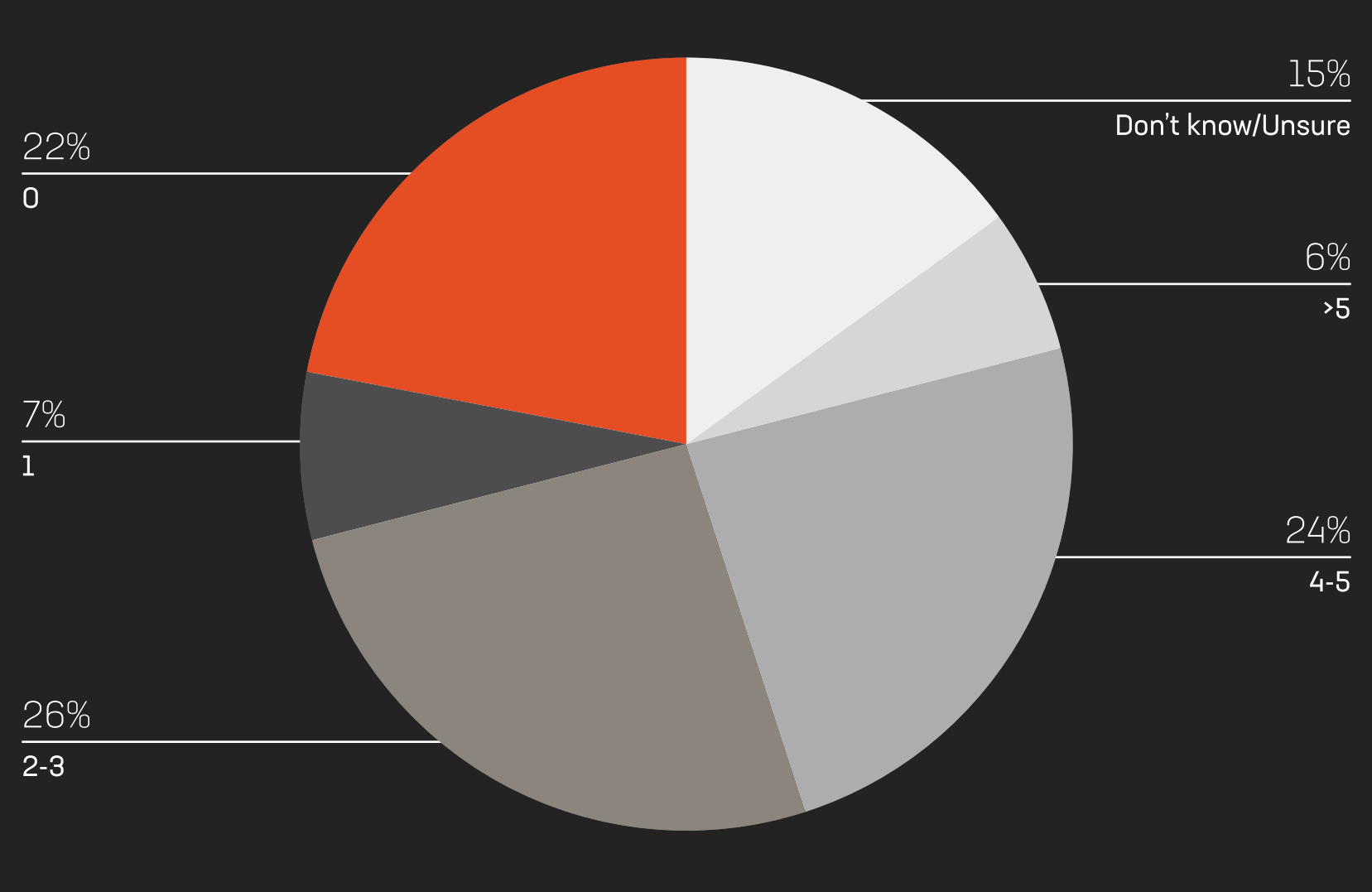
HAS YOUR ORGANIZATION BEEN TARGETED IN A PHISHING SCAM IMPERSONATING YOUR CEO IN THE PAST 18 MONTHS?



Almost half (49%) of executives say that their organization has been targeted in a phishing scam impersonating their CEO in the past 18 months.

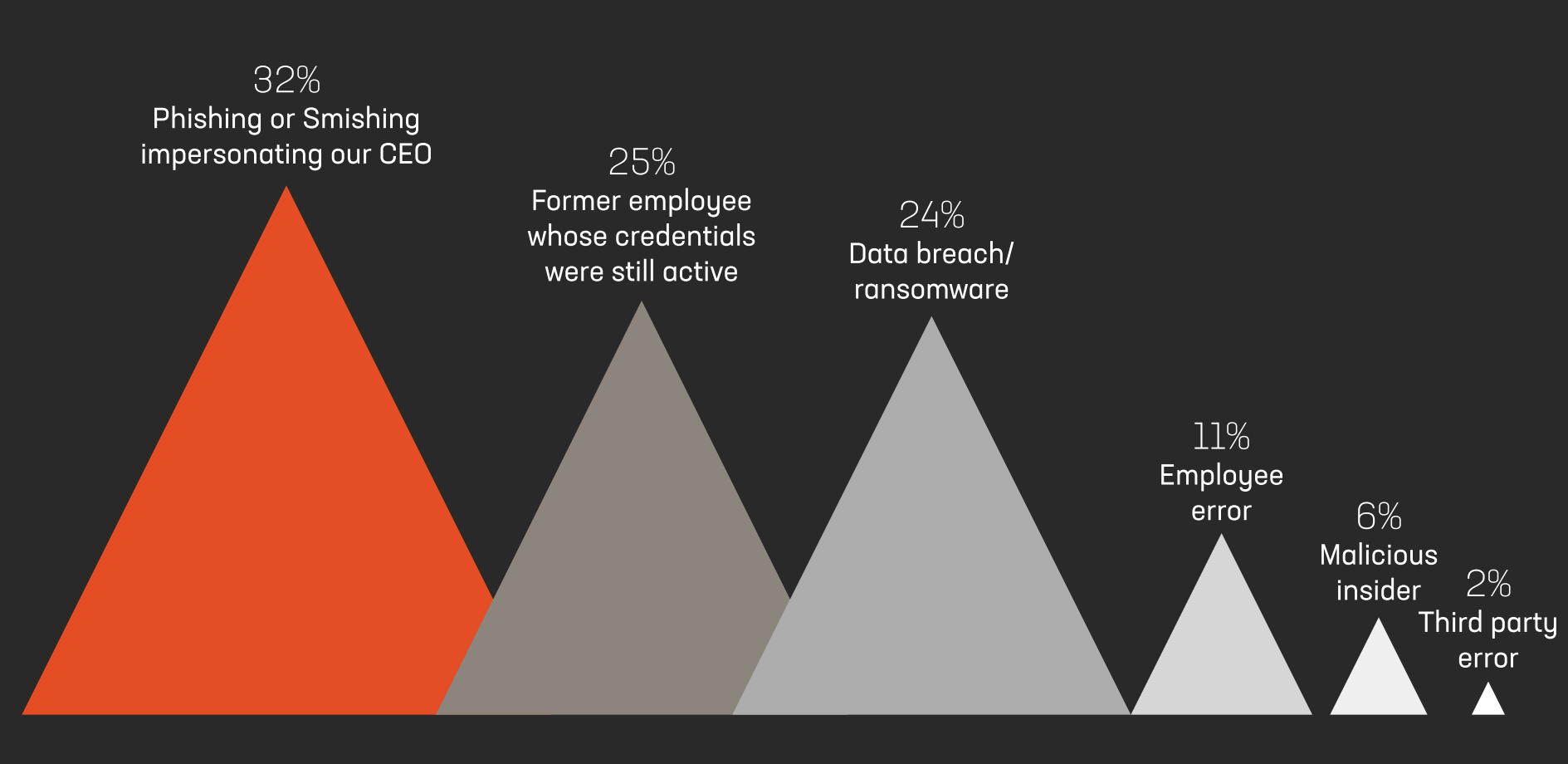
Most respondents have had their executive credentials exposed by bad actors - and only some are actively looking for breached credentials

OVER THE PAST 2 YEARS, HOW MANY TIMES HAVE THE CREDENTIALS OF KEY EMPLOYEES AT YOUR ORGANIZATION BEEN EXPOSED BY CYBERCRIMINALS?



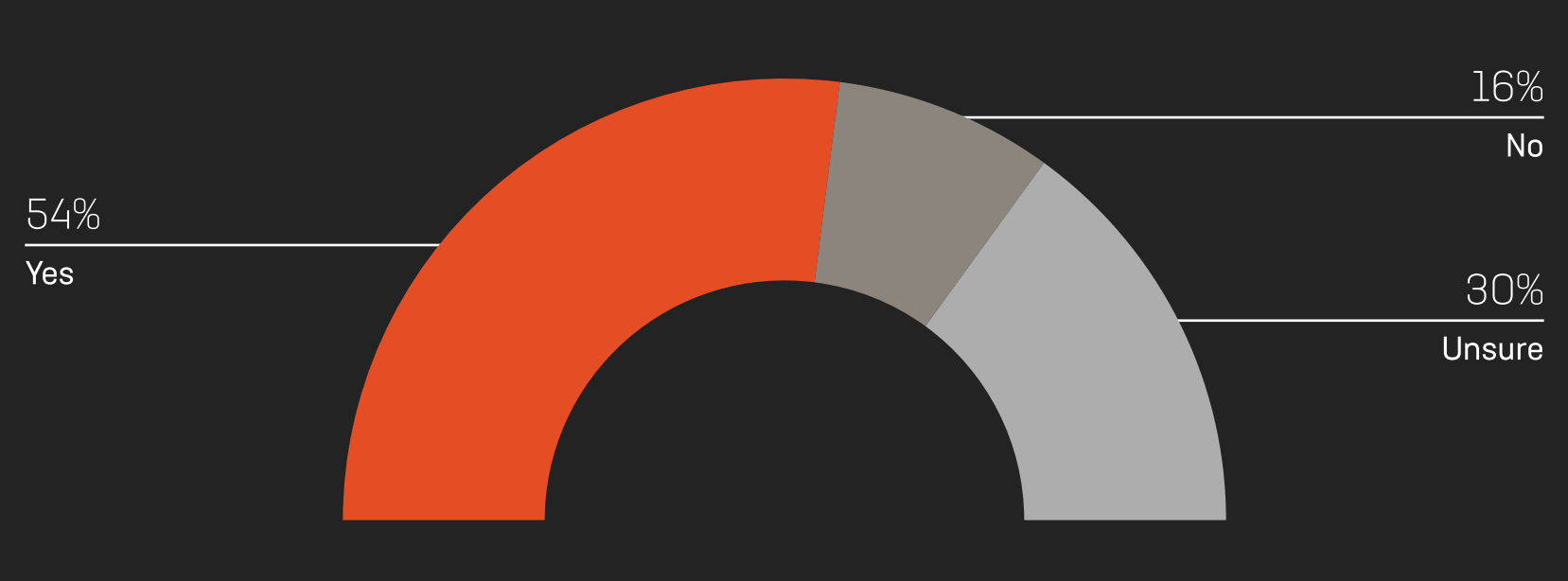
56% of executives say the credentials of key employees have been exposed by cybercriminals at least 2 times over the past 2 years.

WHAT WAS THE ROOT CAUSE OF THE EXPOSED CREDENTIALS?



For those who had exposed credentials, executives say it was due to CEO impersonations (32%), former employees whose credentials were still active (25%), and a data breach or ransomware (24%).

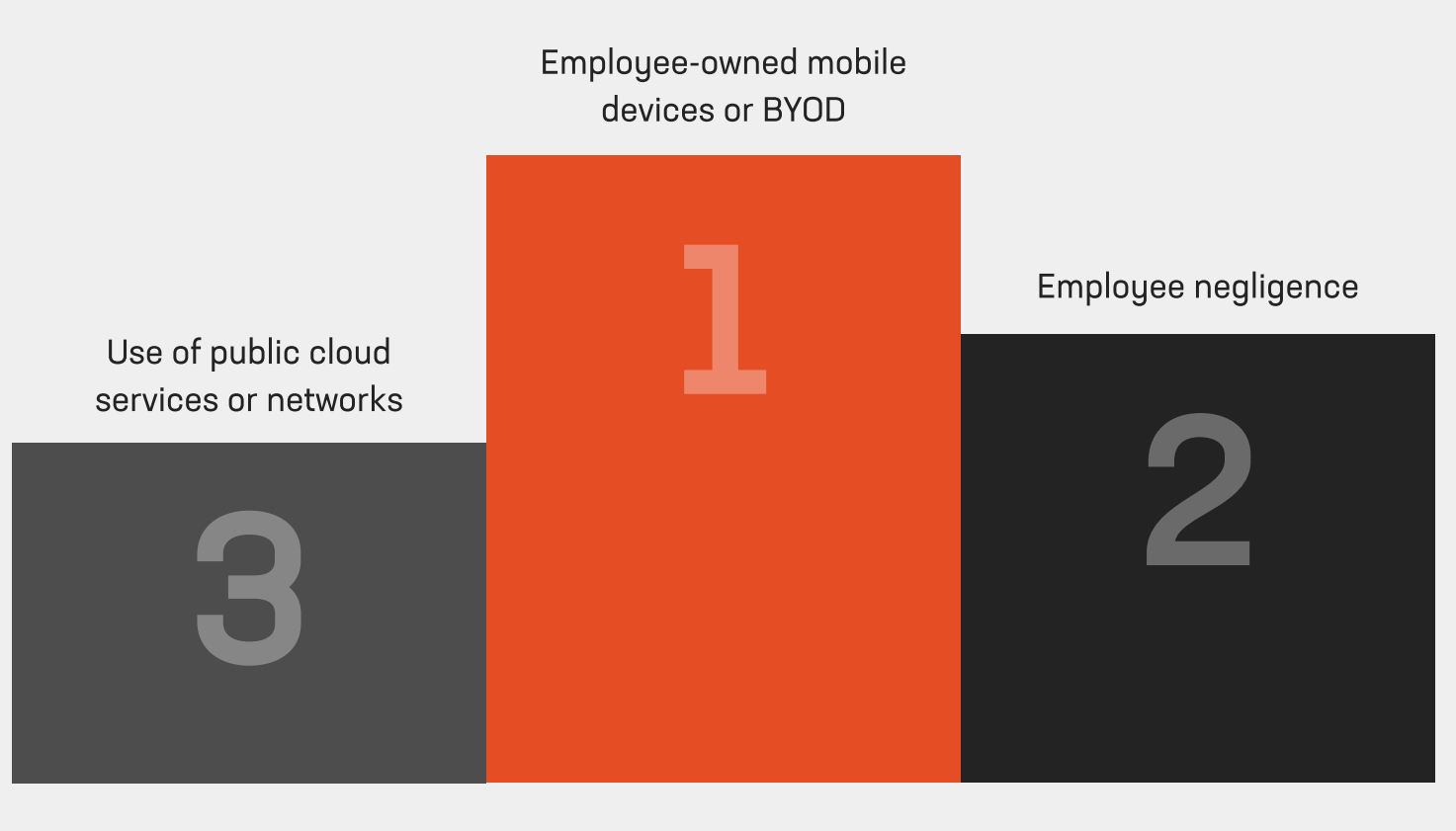
DOES YOUR ORGANIZATION USE SOME COMBINATION OF PEOPLE, TECHNOLOGY, OR SERVICE PROVIDERS TO LOOK FOR (OR MONITOR) KEY EMPLOYEE EXPOSED CREDENTIALS ON THE DARK OR SURFACE WEB?



46% of executives say their organization doesn't (or are unsure if they) monitor key employee exposed credentials on the dark or surface web.

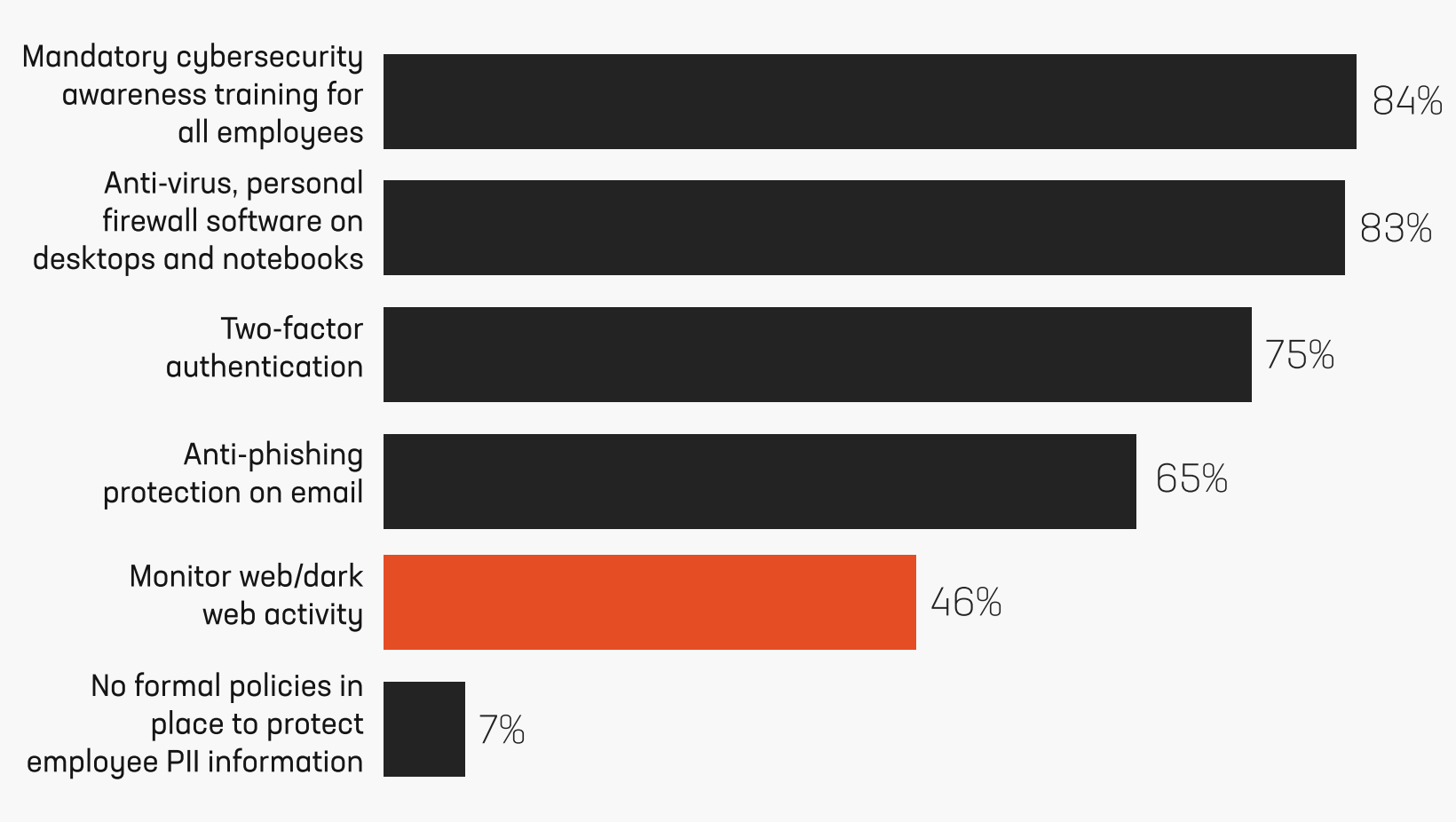
Most executives are concerned about employee-centric threats and are using cybersecurity awareness training and monitoring tools to protect sensitive information

WHAT THREATS TO SENSITIVE & CONFIDENTIAL INFORMATION WITHIN YOUR ORGANIZATION ARE YOU MOST CONCERNED ABOUT?



In terms of threats to sensitive and confidential information, executives are most concerned with employee-owned mobile devices or BYOD, employee negligence, and the use of public cloud services or networks.

WHAT IS YOUR ORGANIZATION DOING TO REDUCE THE LIKELIHOOD OF HAVING AN EMPLOYEE'S PII AND OTHER SENSITIVE DATA COMPROMISED?



Only 46% of companies are monitoring the dark or surface web to protect their employee's PII and other sensitive data.

HOW DOES YOUR ORGANIZATION PROTECT YOUR KEY EMPLOYEES LIKE EXECUTIVES AND PRIVILEGED IT PERSONNEL AGAINST CYBER-ATTACKS THAT TARGET THEIR CREDENTIALS AND PERSONAL IDENTIFIABLE INFORMATION (PII)?

"We perform executive profiling, collect OSINT to monitor the profiles of executives and also use an external service to monitor the same."

- VP, software, 10,001+ employees

"We leverage multiple layers of protection which includes DLP tools, local machine scanning tools, training and ongoing testing to ensure employees understand the risk and help prevent it."

- VP, software, 10,001+ employees

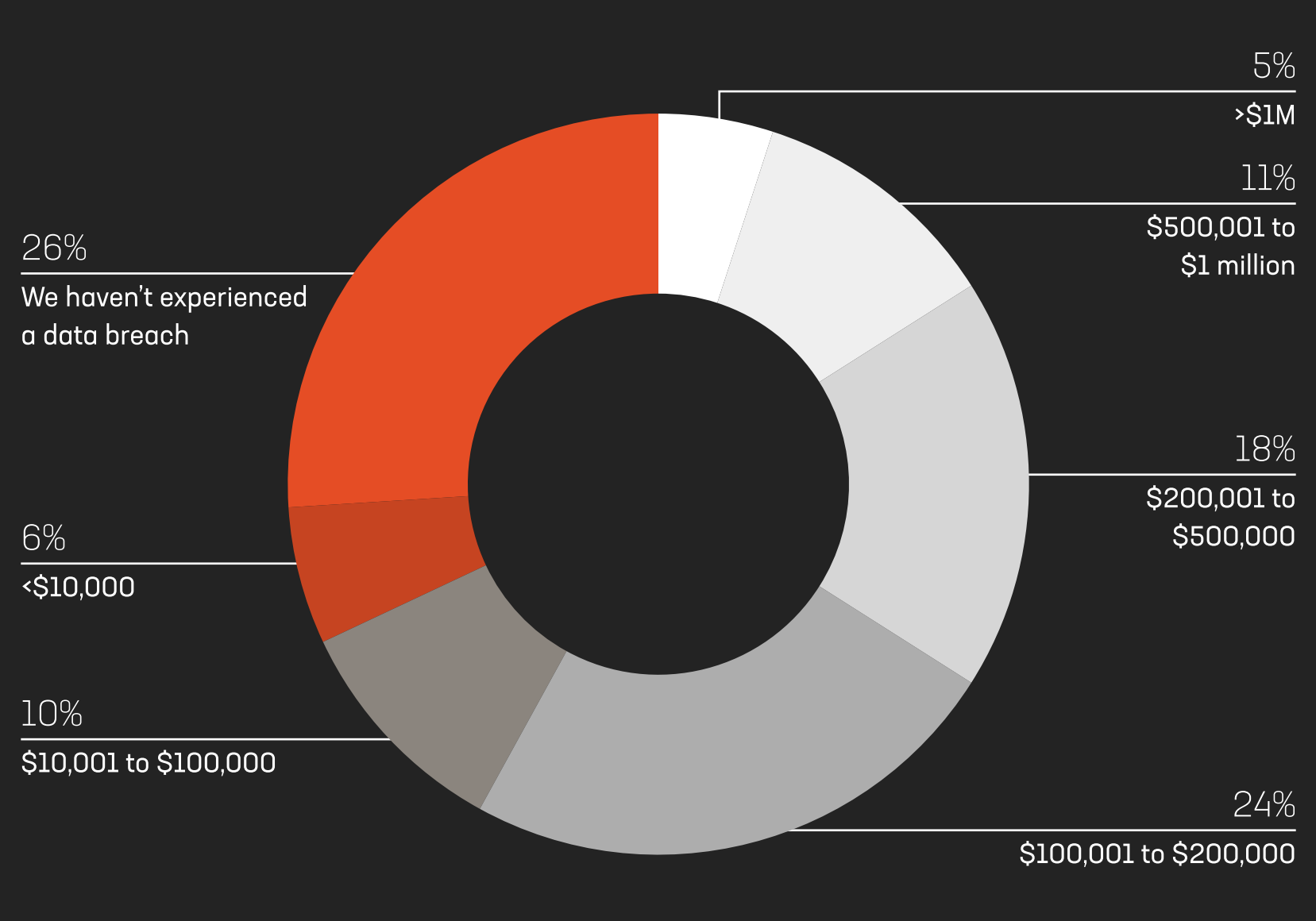
"[We use] multi-factor authentication, limit sensitive/ personal information shared on social media, stronger encryption on emails and hard-drive."

- VP, finance, banking & insurance, 10,001+ employees

Executives say their organization protects their key employees against cyberattacks through multi-factor authentication, monitoring activity, and security awareness training for employees.

Data breaches can have a significant financial impact on enterprise organizations

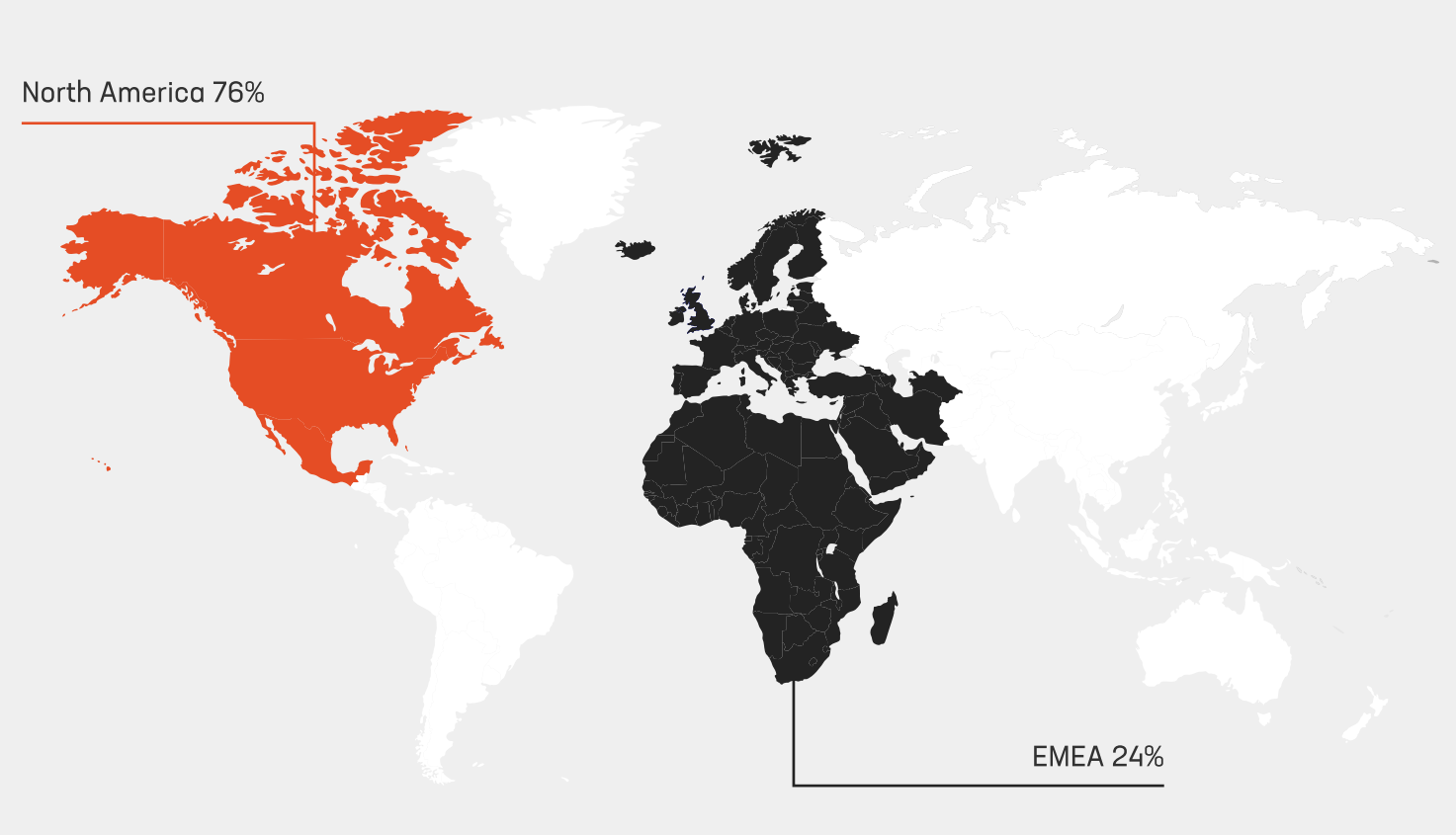
IN YOUR OPINION (BEST GUESS), WHAT IS THE FINANCIAL IMPACT ON YOUR ORGANIZATION WHEN A DATA BREACH OCCURS?



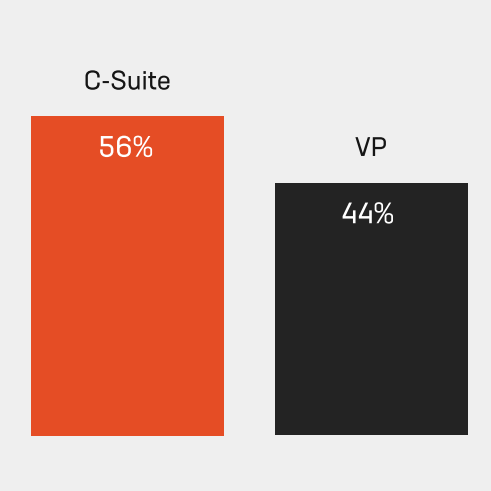
53% of respondents estimate it costs their organization between $100 thousand and $1 million when a data breach occurs.

Respondent Breakdown

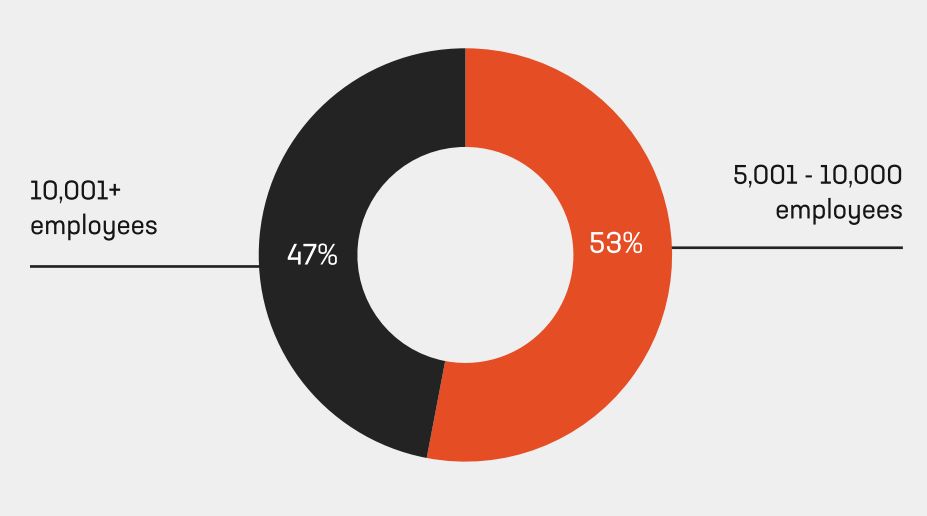
REGION



TITLE



COMPANY SIZE



Insights powered by PULSE