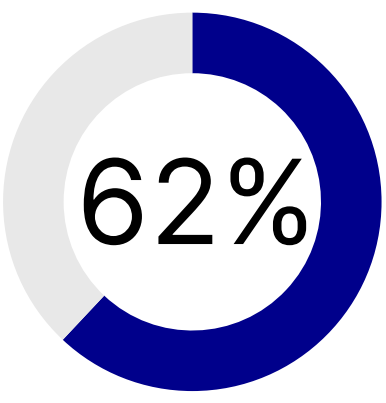
opentext™

Ransom Payments Persist as Supply Chain Attacks Surge

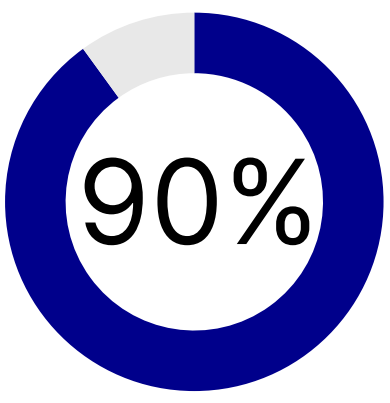
OpenText Cybersecurity's 2024 Global Ransomware Survey

Both small and medium-sized businesses (SMBs) and large enterprises are improving defenses, but face repercussions of ransom payments with about half of respondents experiencing a ransomware attack.

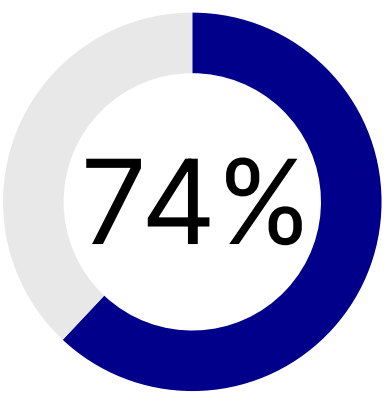
OVERWHELMING CONCERN ABOUT THE EFFECTS OF A SUPPLY CHAIN ATTACK FOR BOTH SMBS AND ENTERPRISES SHOWS A NEED FOR IMPROVED SECURITY PRACTICES



More than half of SMBs and enterprises have been impacted by a ransomware attack originating from a software supply chain partner.

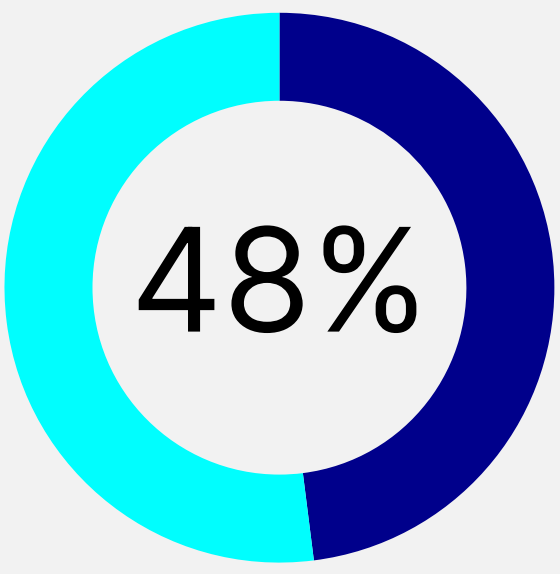


The majority are planning to increase collaboration with software suppliers to improve security practices in the next year.

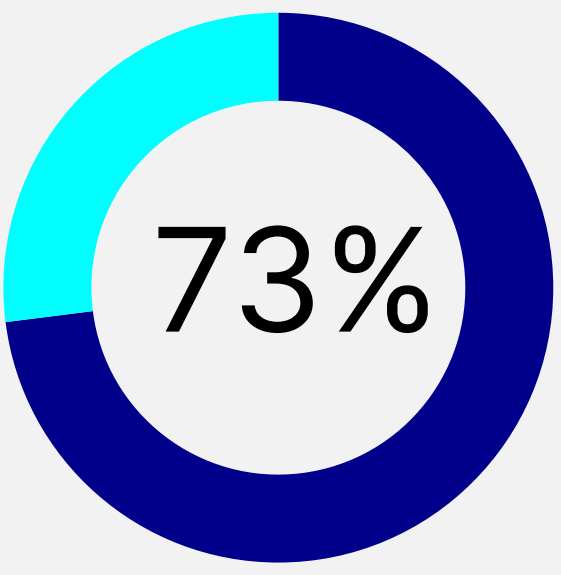


Almost three-quarters, have a formal process for assessing the cybersecurity practices of your software suppliers.

RANSOMWARE ATTACKS PERSIST AS A CRITITCAL THREAT TO SMBS AND ENTERPRISES



Nearly half of SMBs and enterprises have experienced ransomware attacks.



Nearly three-quarters of SMBs and enterprises have experienced ransomware attack **in the last year**.

SMBS AND ENTERPRISES EXPERIENCING MORE PHISING ATTACKS DUE TO THE INCREASED USE OF AI

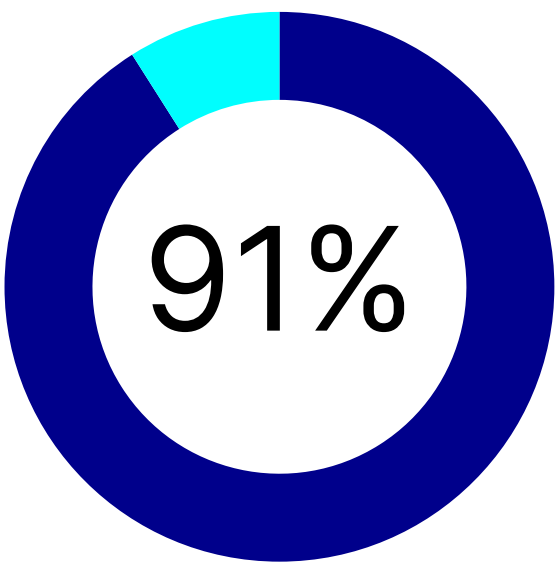
45%

Nearly half of SMBs and enterprises have observed an increase in phishing attacks due to an increased use of AI.

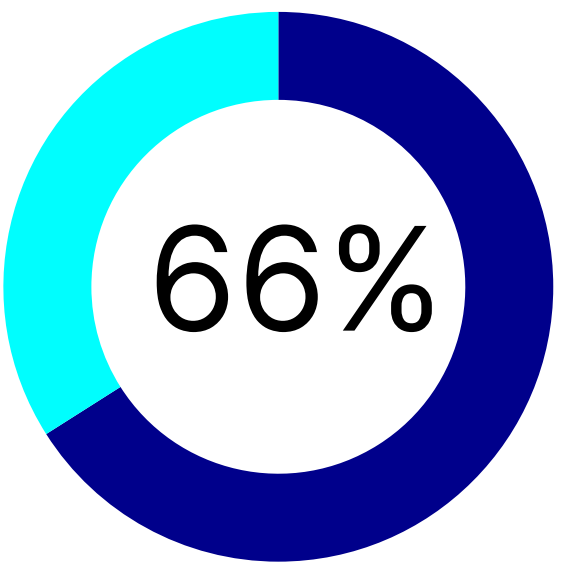
69%

Of those who experienced a ransomware attack, many have observed an increase in phishing attacks due to the increased AI usage.

SMBS AND ENTERPRISES CONTINUE TO INVEST MORE IN CLOUD SECURITY AND SECURITY AWARENESS AND PHISHING TRAINING.



The majority of SMBs and enterprises require employees to take security awareness and phishing training.



In **2024** more than half of SMBs and enterprises conducted training **at least quarterly**.

Survey Methodology
OpenText Cybersecurity polled 1,781 c-level executives, security professionals and security and technical directors from SMBs and enterprises in the United States, the United Kingdom, Australia, France, Germany and India from August 23 to September 10, 2024. Respondents represented multiple industries including technology, financial services, retail, manufacturing, healthcare, education and more.

About OpenText Cybersecurity
OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified/end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

opentext™ | Cybersecurity