Combatting the Escalation in Business and Vendor Email Compromise

Business Email Compromise (BEC) is a sophisticated cyberattack where cybercriminals defraud organizations for financial gain or sensitive information. BEC attacks are among the most financially damaging cybercrimes globally, with average losses estimated to be 80 times greater than those incurred from ransomware. According to the FBI's Internet Crime Complaint Center (IC3), BEC incidents and financial losses have risen dramatically: from 467,361 incidents and $3.5 billion in losses during 2019 to 880,418 and $12.5 billion in 2023. With an average loss exceeding $125,000 per incident and worldwide losses totaling $50.8 billion, BEC attacks now pose a threat not only to individuals but also to the critical infrastructure and economies of countries on a global scale. To combat this growing menace, organizations must adopt a proactive approach by implementing robust defensive security measures and arming themselves with knowledge to mitigate these attacks.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.