HYCU®

HYCU.COM

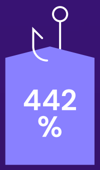
3 Cybercrime Trends Impacting IT Leaders in 2025

1

AI Will Transform Social Engineering

Change

Gone are the days of easy-to-find phishing emails. GenAI is giving bad actors video, image, voice cloning capabilities and the power of creative agencies to launch the perfect social engineering campaign.



442% increase in phishing Attacks due to GenAI[1]

Impact on IT

Higher conversion rates are leading to successful credential access and privilege escalation. This will require immutable, offsite copies of all critical workloads, from production applications to the rest of the technology stack.

2

SaaS Applications Are a Top Target

Change

AI-supercharged attackers will successfully access SaaS accounts – especially business applications outside of IT that contain critical customer and employee data (HR, Finance, Sales, etc.)

Impact on IT

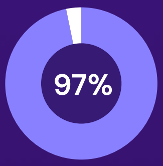
High ROI, low hanging fruit applications will require IT to step in and ensure data is protected and recoverable.

3

Software Supply Chain Attacks Will Rise

Change

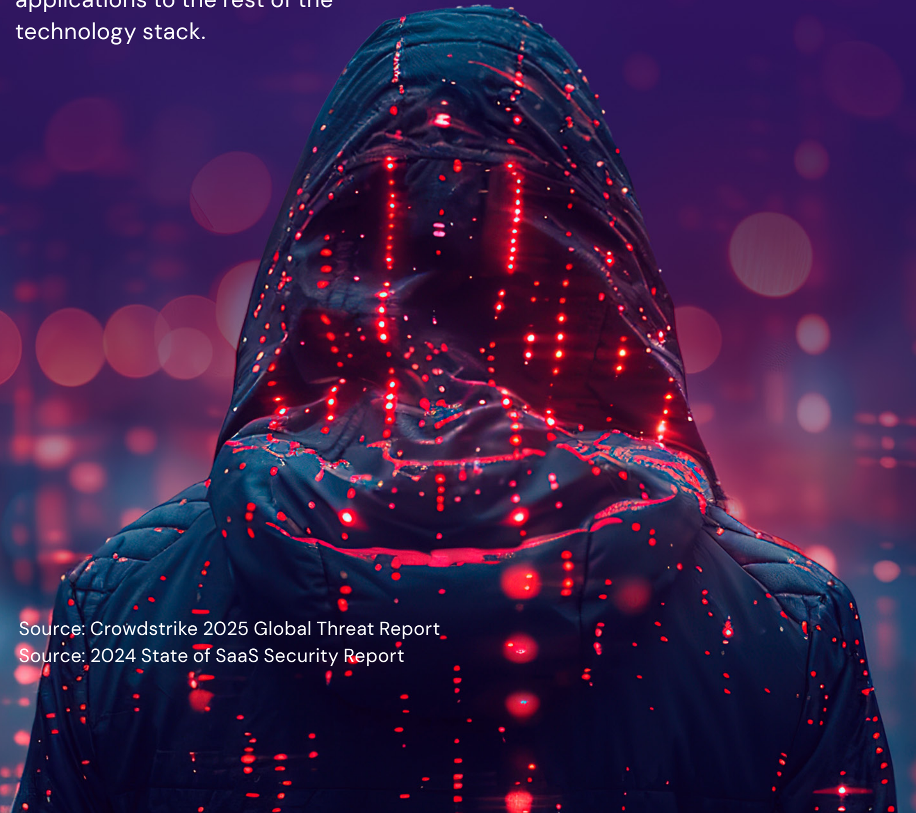
SaaS providers, especially rapidly growing ISVs, are prime targets.



97% of organizations faced exposure to attacks through compromised SaaS supply chain applications[2] and recent attacks on Snowflake, GitHub, MOVEit show that no vendor is infallible.

Impact on IT

IT must deliver business continuity plans to ensure critical access to SaaS data in case of prolonged outages or permanent data deletion in a supply chain attack.



Stay ahead of the game

Download checklist

[1] Source: Crowdstrike 2025 Global Threat Report
[2] Source: 2024 State of SaaS Security Report