HACK3R_
RANGERS

CYBERSECURITY TRENDS FOR 2026

1

Forecast of a

40%

increase in ransomware victims in 2026

Source: QBE Report, 2025

RANSOMWARE

Ransomware continues to be one of the main attack vectors in 2026 and the number one concern of CISOs worldwide (Global Cybersecurity Outlook, 2026).

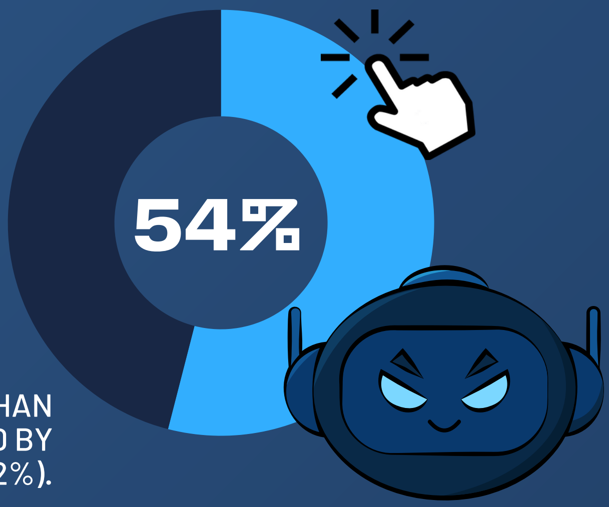
After all, data extortion tactics are becoming more aggressive, and an interruption to critical operations can mean millions in losses.

2 AI-DRIVEN THREATS

GenAI is already making social engineering attacks more accurate, personalized, and harder to detect. In addition, with the advancement of autonomous AI agents capable of operating at scale, the threat landscape is entering a new level.

AI-generated phishing emails achieve click-through rates of up to 54% (2025 Global Threat Report, Crowdstrike).

CLICK-THROUGH RATE OF AI-GENERATED EMAILS



4X HIGHER THAN MESSAGES CREATED BY HUMANS (12%).

3

EXPANSION OF THE ATTACK SURFACE TO IOT, OT, AND EDGE

67%

of expansion in the attack surface across IoT, OT, and edge devices.

Source: TechTarget

The increased use of Internet of Things (IoT) devices and cloud services is **expanding the attack surface and introducing new vulnerabilities**.

Cloud technologies are identified as the **second biggest factor** impacting cybersecurity risks in 2026, second only to Artificial Intelligence. *(Global Cybersecurity Outlook, 2026)*

Attacks evolve every year. And your company's defense needs to keep up. Hacker Rangers turns your employees into the strongest link in security.

ACCESS HACKERRANGERS.COM AND GET A DEMO