

# Major Attacks on Telecom Infrastructure

SecAwarenessTruss Training Framework for Critical Infrastructure Defence

## SecAwarenessTruss Cyber-Range

Dynamic Training | Cross-Sector Scenarios | Hands-on Learning

Data compiled from 2024-2026 threat intelligence reports | EU Digital Europe Programme



### DDOS ATTACKS

Massive distributed denial-of-service attacks overwhelming telecom infrastructure with unprecedented scale and velocity.

**8M+**

ATTACKS H1 2025 GLOBALLY

**5-10 Tbps**

PEAK ATTACK RANGE (NEW NORMAL)

**37%**

ATTACKS COMPLETE IN <2 MINUTES

●●● CRITICAL



### SIM SWAPPING

Account takeover fraud exploiting weak telecom authentication and social engineering to hijack phone numbers and intercept OTPs.

**240%**

SURGE IN 2024 (VS 2023)

**\$50M+**

LOSSES FROM 1,075 ATTACKS (2023)

**90%**

OCCUR WITHOUT VICTIM INTERACTION

●●● CRITICAL



### SUPPLY CHAIN ATTACKS

Sophisticated breach of telecom suppliers, vendors, and infrastructure providers with cascading effects across ecosystem.

**63%**

TARGET IT/TELECOM SECTOR

**Doubled**

INCIDENTS SINCE APRIL 2025

**10M+**

CUSTOMERS AFFECTED (OPTUS INCIDENT)

●●● HIGH

## SecAwarenessTruss Training Framework

#### Risk Assessment

Cyber risk and impact assessment framework driving targeted training scenarios for telecom sectors

#### Sector-Specific Focus

Tailored training for telecom, energy, health, and maritime critical infrastructure organizations

#### Gamification

Interactive exercise scenarios with gamification elements for hands-on learning and engagement

#### Collaborative Response

Cross-sector complex scenarios enabling coordinated incident response and knowledge sharing

#### Threat Intelligence

Common data repository and threat intelligence sharing among cybersecurity ranges

#### Defense Readiness

Systematic training programs for cyber defence workforce development and proactive threat management

## 2025 Attack Statistics Snapshot

DDOS ATTACKS YOY GROWTH

**+358%**

TELECOM SECTOR DDOS TARGET RATE

**16%**

SIM SWAP UK INCREASE (2023-24)

**1,055M**

SUPPLY CHAIN TARGET %

**63%**

TECOM OPS W/ LIVING OFF LAND

**63%**

LAYER 7 DDOS ATTACKS

**80%**

## Major Incidents & Escalation Timeline

#### 2023-2024 FBI SIM Swap Investigations

1,075 SIM swap attacks investigated by FBI in 2023, resulting in ~\$50M in losses. 240% surge in 2024 continues threat escalation.

#### 2024 Salt Typhoon Campaign

Major cyber espionage campaign targeting U.S. telecommunications infrastructure. Long-term, stealthy infections exposing massive vulnerabilities in core telco systems.

#### Sept 2025 U.S. Secret Service SIM Server Bust

Dismantled sophisticated telecom threat network with 300+ co-located SIM servers and 100,000+ SIM cards capable of cell tower disruption and DoS attacks.

#### Q1 2025 DDoS Surge & Layer 7 Dominance

Cloudflare blocked 20.5M DDoS attacks in Q1 2025 alone. 80% targeting Layer 7 with attacks reaching 859M requests (+270% vs Q1 2024).

#### H1 2025 Netscout Global Monitoring

8M+ DDoS attacks monitored globally, with 3.2M in EMEA region alone. Terabit-scale attacks now daily reality (vs once every 5 days in 2024).