

2025 OAD REPORT EXECUTIVE SUMMARY

ED.BY MARCO R. A. BOZZETTI

in collaboration with:



Silver Sponsor



Preface by:

Massimo Di Virgilio, FIDAInform President

Ivano Gabrielli, Director of the Postal Police and Cybersecurity Service

Antonio Piva, AICA President

OAD 2025 Executive Summary

The Osservatorio Attacchi Digitali in Italia (OAD – Observatory on Digital Attacks in Italy), with this 2025 edition, reaches its eighteenth consecutive year of research on digital attacks and security measures in information systems across Italy. As in previous years, the OAD benefits from the valuable collaboration of the Italian “Postal and Cyber Police Service,” which contributed data and the content of Chapter 8 of this Report.

To download the Report OAD 2025 (in Italian): <https://www.aipsi.org/eventi/eventi-in-programma/992-pubblicato-e-liberamente-scaricabile-il-rapporto-oad-2025-di-aipsi.html>

The OAD 2025 online survey refers to intentional attacks detected in Italy IT systems (IS) throughout the entire year 2024 and highlights the continued widespread and serious prevalence of digital attacks, with significant impacts on IS of the responding organizations and companies.

The year 2024 witnessed a worsening of the global geopolitical situation, with ongoing "hybrid" wars, particularly due to the invasion of Ukraine and the Palestinian issue. Alongside military interventions and clashes—more and more reliant on drones and aircraft—there has been a rise in digital attacks targeting the Information Systems (IS) of public and private entities in countries directly or indirectly involved in these conflicts. This was accompanied by a significant increase in disinformation campaigns, not only regarding the ongoing wars but also on social, political, and religious topics.

In 2024, Artificial Intelligence (AI) techniques were extensively used in various digital attack tools, as well as for disinformation purposes.

Chapter 3 outlines the global digital threat landscape, referring to the World Economic Forum (WEF) and the ENISA's (European Union Agency for Cybersecurity) annual Threat Landscape (ETL) reports, as well as the Italian ACN (National Cybersecurity Agency) and the Postal and Cyber Police Service. The OAD 2025 survey introduced AI as both an attack target and a tool, and provided vertical analyses of web systems, OT (Operational Technology) systems, and AI-based systems.

Respondents numbered in the hundreds, mainly ICT solution providers (21.4%), followed by manufacturing and construction (14.85%), healthcare and social services (14.41%), and business support services (10.48%). SMEs represented 62.96% of respondents, with 22.22% micro-enterprises (<10 employees). OAD remains unique in its consistent inclusion of SMEs (over 60% every year).

Respondent roles were mainly owners/executives (26.22%), CIOs (22.56%), and cybersecurity or IT specialists, either independent consultants or employees of specialized firms, to whom the organization had outsourced, fully or partially, the management of their ISs and/or security. This confirms the ongoing outsourcing trend. Fewer than 10% were CISOs, CSOs, or CTOs.

Throughout 2024, **71.18%** of the responding organizations experienced digital attacks on their IS.

The most common **types of attacks** among the 16 families considered included:

- Malicious or unauthorized modifications to ICT system programs and configurations, reported by 29.26% of respondents; this top position is surely influenced by the widespread presence of malware and ransomware in Italy;

- Unauthorized and malicious use of the ICT systems of the IS as a whole, at 23.58%;
- DoS/DDoS attacks, aimed at saturating ICT systems connected to the Internet, at 20%; these were among the most frequently used attacks in cyber warfare, particularly by pro-Russian hacker groups;
- Supply chain attacks (14.85%), a major global risk per WEF;
- AI-based system attacks (7.86%).

Regarding **attack techniques** likely used in the most severe digital attack suffered, among the 8 families of techniques considered, the 2025 survey highlights the following most frequent:

- 37.12% reported the use of multiple attack techniques, simultaneously and/or in parallel;
- 15.72% involved illegal information gathering, including social engineering;
- 10.04% involved malicious code, the basis of the highly prevalent ransomware attacks.

“Vertical” analysis of the most severe attacks revealed:

- for **web systems**:
 - 94.15% use both on-premise and outsourced web systems;
 - 58.4% detected attacks on applications and web environments, 60.6% of which affected cloud systems;
 - technical vulnerabilities caused 93.83% of the most severe attacks, often linked to human error (44.44%);
 - referring to the top 10 OWASP web vulnerabilities, outdated/vulnerable software ranked first (39.51%), followed by misconfiguration (30.86%) and identity/authentication failures (25.93%);
 - the technical impact was significant, with 64.29% of cases experiencing service disruption lasting two or more days;
 - the economic impact was also significant, with increased costs on the IS budget reported by 86.5% of respondents, and for 12.36%, these costs also affected the company balance sheet;
 - sabotage (44.44%), fraud (40.74%), and extortion (~30%) were the top motives, while hacktivism (21%) and cyberwarfare (16%) showed rising geopolitical influence;
- for **OT environments** :
 - used by 40.58% of respondents; 32.1% attacked;
 - robotic systems were most affected (70%), followed by IoT/IIoT (55.56%);
 - 85% reported downtime >2 days, often spreading to IS applications (30% for 2–3 days);
 - the economic impact of the most severe attack was also significant: 37% on IS costs/budget, and 30% with repercussions also on the company balance sheet;

- the (probable) motivations for the most severe attack placed sabotage first at 93%, followed by vandalism at 37%, and extortion at 22%;
- for **AI-based systems**:
 - 41% already use AI applications; 23.8% faced digital attacks;
 - based on OWASP Top 10 for AI (LLMs and GenAI), “Data and Model Poisoning” (35%) and “Improper Output Handling” (20%) were the main vulnerabilities;
 - most AI vulnerabilities relate to “prompt” inputs and model training methods—partially regulated by the EU AI Act.

The IS of 87.57% of respondents is managed entirely in Italy; 61.58% operate without a Data Center, typical of SMEs. For 75.14%, the IS is critical to business continuity, and 25.42% provide NIS2- essential/critical services. Full outsourcing applies to 24.29% (IS management) and 27.43% (IS security), while 42–46% adopt partial outsourcing, confirming a strong trend toward managed cybersecurity services.

40% of respondents completed the optional section on digital security measures. Among these, 40.3% declared adequate and 46.8% high levels of IS security, with only 12.9% insufficient and none critical.

Key findings on organizational, technical, and control measures among this 40% sample include:

- Organizational Security Measures:
 - 80% have digital security policies and procedures;
 - 92% use user support tools;
 - 81% conduct digital risk assessments;
 - 52.38% perform audits;
 - 38% hold digital security certifications.
- Technical Security Measures:
 - 67.14% maintain high IS reliability;
 - 85.71% control physical access to ICT premises;
 - 79.1% use UPS systems;
 - 80.8% centrally manage passwords;
 - 57.58% monitor network performance and security;
 - 33.85% adopt secure software development practices;
 - 80% deploy application firewalls (FWA);
 - 84.7% manage corrective maintenance;
 - 43.75% follow backup best practices;
 - 76.56% apply recovery procedures.
- Management and Control Measures:
 - 81.25% have centralized IS control systems;
 - 78.79% manage IT supply chains;

- 80% conduct vulnerability analyses;
- 80.6% archive logs (46.27% also manage them);
- 70% have Disaster Recovery plans; of these, 70% have tested alternatives.

Despite this maturity, cyberattacks remain widespread and impactful, underscoring that even advanced security systems cannot fully prevent digital incidents.

OAD 2025 confirms global findings by WEF, ENISA, ACN, and the Postal and Cyber Police Service: **systemic digital insecurity**, ongoing since 2018, **now defines the global landscape**.

The imperative is no longer full prevention but resilience — strengthening defenses while ensuring business continuity and tested Disaster Recovery capabilities to manage unavoidable insecurity.



**With the free patronage
of the following Associations**



Anitec-Assinform



ASSOCIAZIONE
SPECIALISTI
SISTEMI
INFORMATIVI



ASSOCIAZIONE Data Protection Officer



Security by Sharing

