
OAD
Osservatorio
Attacchi Digitali
in Italia
aipsi
2024 OAD REPORT
EXECUTIVE SUMMARY
ED.BY MARCO R. A. BOZZETTI
in collaboration with
AICA
FIDA
malabo
ICT Advisory
Silver Sponsor
QINTESI
Preface by:
Ivano Gabrielli, Direttore Polizia Postale e delle Comunicazioni
Alessandro Musumeci, Capo della Segreteria Tecnica del Sottosegretario
all'Innovazione Tecnologica

The **OAD** (Digital Attack Observatory) **2024** marks the **seventeenth consecutive year** of surveys on cyber attacks and cybersecurity measures in Italy. This edition benefits from the cooperation of the Italian Postal Police, which contributed data and authored Chapter 8 of this Report.
The OAD 2024 survey covers intentional cyber attacks detected throughout 2023, underscoring the ongoing and widespread impact of these attacks on the IT systems of the public and private companies participating this survey.

The year 2023 was marked by a worsening global geopolitical landscape, with cyber warfare associated with events such as the Russian Federation's invasion of Ukraine in February 2022 and the defense efforts that followed. Additionally, the conflict between Israel and Hamas, escalated following Hamas' terrorist attack on Israel on 7 October 2023.
These conflicts are part of a broader geopolitical crisis that has sparked numerous cyber attacks, alongside a significant increase in misinformation and disinformation. Furthermore, AI techniques have been increasingly utilized in cyber attack tools. Alongside traditional cybercrime, these factors have contributed to a persistently high number of intentional digital attacks in 2023, with significant impacts on the budgets for cyber security and, in some cases, the financial health of the attacked organizations.

In Chapter 3, the OAD 2024 Report offers a comprehensive overview of digital attacks on a global scale, with references to the World Economic Forum, and at a European level, citing reports from ENISA, the European Union Agency for Cybersecurity (see §3.1). It also highlights examples of some of the most significant attacks carried out in 2023 (see §3.2). On a national level, in addition to the findings from the OAD 2024 online survey—central to the report and detailed in Chapter 4—the Report examines key data from the annual report to Parliament by ACN, the National Cybersecurity Agency (see §3.3), as well as insights provided by the Italian Postal Police (see Chapter 8).

The OAD 2024 online questionnaire included only two questions about all the digital attacks suffered in 2023 by the IT systems of the responding companies. This approach aimed to continue analyzing general attack trends (what is targeted and the techniques used) from 2007 to the present.
It also delves into the specific digital attacks detected in 2023 on **web applications** and on **OT** (Operational Technology) systems.
OAD makes a clear distinction between what is targeted—the type of attack, categorized into 15 different macro-categories—and how it is attacked, referring to the techniques used, classified into 7 macro-categories (for methodological details refer to Annex A).
Throughout 2023, 72.4% of the responding companies reported experiencing digital attacks on their IT systems. The most widespread types of attacks include:

- Malicious/unauthorized modifications to ICT programs and configurations (31.7% of responses), largely driven by the widespread presence of malware and ransomware in Italy.
- DoS/DDoS attacks (20.7%), which overload ICT systems connected to the Internet. These attacks were frequently used in the context of cyber warfare, particularly by hacker groups aligned with Russia.
- Unauthorized and malicious use of ICT systems (18.3%).
- Attacks on the computerized supply chain (15%). This data highlights its prevalence and criticality, aligning with the World Economic Forum's classification of this as a major global risk.
- Theft of mobile devices (13.4%), mainly smartphones. These devices often store valuable digital identity information, such as passwords and access methods, without sufficient protection, making them attractive targets. Additionally, smartphones have significant value on the second-hand market, providing further incentive for theft.

All other types of attacks listed in the OAD taxonomy recorded percentages below 10%. For the first time in OAD 2024, access control systems and network attacks are no longer at the top of the ranking for the most widespread types of attacks, as they were in previous editions.

The most widespread cyber attack's techniques in the most serious attacks see at the top:

- The use of multiple techniques in a single attack, reported by 40.4% of respondents.
- Illegal information gathering, often achieved through social engineering, at 37.6%.
- Malicious code, a core component of the widespread ransomware attacks, at 25.3%.

The correlation of data on detected attacks with the size of the company (as number of employees) confirms that in 2023, the largest and wealthiest organizations were the primary targets of the most frequent and sophisticated digital attacks. Small and very small organizations, whether private or public, are generally not of specific interest to cybercriminals in targeted attacks. However, they can still become victims of mass attacks, such as those based on phishing and ransomware.

The 2024 "vertical" survey on attacks targeting web applications (outlined in §4.2) was based on analyzing the causes of the most severe attacks, focusing on the main vulnerabilities and risks identified by OWASP. Given that most applications are web-based, and many are hosted in the cloud, modern IT system, regardless of their size, tend to be partially on-premise and partially on one or more clouds from different providers (multi-cloud). This prompted a deeper investigation into the technical causes of attacks experienced by the survey's responding companies. From this data, 58.4% of respondents reported detecting attacks on web applications and environments, and of these, 60.6% suffered attacks within their cloud environments—despite the expectation that cloud environments are generally more secure than on-premise systems. The vulnerabilities that caused the most severe attacks were attributed 92.3% of the time to human factors, which also partially reflect organizational shortcomings (such as inadequate user training), and 82.7% to technical issues.
When referencing OWASP's top 10 web vulnerabilities, the most serious attacks identified by respondents were primarily caused by outdated and vulnerable software components, ranking first at 31.7%. This was followed by misconfiguration of security tools at 20.4%.
The OAD 2024 questionnaire also addressed the 10 main risks related to API interfaces in web environments as identified by OWASP. Around 50% of the respondents stated that the most serious attack they experienced was not caused by any of the OWASP top ten web API risks. Among the remaining respondents, API security misconfiguration emerged as the leading cause, aligning with the findings on web vulnerabilities.
The impact of the most serious attack on web environments was severe for the IT systems of the respondents. In 85.3% of cases, the attack resulted in a disruption lasting two days or more. Economically, the impact was also significant, with 86.5% reporting increased costs to their IT system budget, and 24% noting that these costs extended to affect the broader budget of the company.
Regarding the motivations behind the most serious attacks, nearly two-thirds of respondents cited economic reasons, such as fraud and blackmail. Notably, for the first time in OAD's history, cyber warfare ranked third among attack motivations, reported by 20.2% of respondents.

The 2024 "vertical" survey on attacks targeting OT (Operational Technology) systems, detailed in §4.3, included only those respondents that reported using OT systems, accounting for 37% of the total. Among these, 48.2% confirmed experiencing attacks on their OT systems.
The impact of the most serious OT attack was significant, particularly in terms of system downtime. For approximately one-third of respondents, the system was blocked for 2 to 3 days, while for nearly half, the downtime exceeded 3 days. Given that most modern OT systems are interconnected with the centralized applications of the IT system, these disruptions extended to some IT systems as well. As a result, 40.7% of respondents reported that centralized IT applications were also blocked for 2 to 3 days due to this cross-system impact.

The findings of the OAD 2024 survey are largely consistent with those reported by key organizations such as the World Economic Forum, ENISA (European Union Agency for Cybersecurity), ACN (National Cybersecurity

Agency), and the Italian Postal Police. The latter contributed data on cybercrime detected during 2023 and the first half of 2024, which are detailed in Chapter 8 of this Report.

To provide a clearer understanding and context for the findings on digital attacks, OAD conducts an extensive analysis of the responding companies. This includes the type of company (§6.1), the nature and importance of their IT systems for their operations or business (§6.2), and the cybersecurity measures they have implemented. The pool of respondents encompasses a wide range of sectors, including Public Administrations. The most represented sectors are:

- Education, with 23.6% of respondents,
- Professional and business support services (including lawyers, accountants, notaries, etc.), accounting for 12.3%,
- Manufacturing and construction industry, which makes up 11% of the total respondents.

In terms of company size, based on the number of employees, 69.8% of the respondent companies are small and medium-sized organizations, defined as those with fewer than 250 employees. Notably, 22.9% of the respondents are organizations with fewer than 10 employees, reflecting the structure of the Italian economy, where such small businesses make up the vast majority of companies.

For 70.1% of the responding companies, the IT system plays a crucial role in supporting their activities and processes, underscoring the need for robust, effective, and efficient digital security. Additionally, 10.6% of the respondents provide essential services for Italy, making them subject to the NIS Directive and soon to new European regulations such as NIS2 and DORA.
Among the respondents, 85.4% manage and control their IT systems entirely within Italy, with 63.4% having small-to-medium-sized systems without a dedicated Data Center. A vast majority, 92%, rely on outsourced ICT services, particularly in the cloud.
Regarding operational management, 24.4% of respondents handle it entirely in-house, while 38.6% fully outsource it and 37.1% partially outsource certain aspects. When it comes to the management of digital security, 20% of respondents manage it internally, but 80% outsource it—41.6% completely. This high percentage of fully outsourced digital security management is significant, as smaller organizations typically lack the resources to manage security independently and must turn to consultants or specialized companies for support.

In the OAD 2024 questionnaire, the questions regarding the measures for cybersecurity were optional, and 35.4% of respondents provided answers. The data, detailed in Chapter 7, indicates that most respondents show good levels of both technical and organizational cybersecurity. This positive outcome likely reflects the higher participation of companies with more robust security systems, as those with weaker security measures may have been less inclined to respond.
However, some security deficiencies were more prevalent, particularly among smaller organizations, especially in organizational aspects. Many of these smaller entities also rely on outsourced services for managing their digital security.

While the majority of responding companies are positioned within the higher range for digital security measures, they still experienced numerous digital attacks. These attacks resulted in significant disruptions and incurred substantial costs for their IT systems and, in many cases, for the entire economic budget.

In summary, throughout 2023, serious digital attacks and significant cyber risks continued to spread globally, across Europe, and in Italy.
In Italy, we have been in the era of *systemic digital insecurity* since 2020, and this reality affects the entire world. Despite the implementation of security measures—often at substantial cost—these defenses have not been sufficient to stop digital attacks. With the current available measures, which must be strengthened

rather than abandoned, **companies need to learn how to manage this insecurity through resilience strategies**.

On the business side, resilience can be ensured through *business continuity*—the ability to maintain the operation of critical processes. On the IT side, resilience requires an effective, actionable, and thoroughly tested *Disaster Recovery* plan. These are essential tools to navigate the persistent insecurity and maintain functionality in the face of digital threats.