OAD
Osservatorio
Attacchi Digitali
in Italia

PROPOSAL OF
SPONSORSHIP
OAD 2024

AN INIZIATIVE OF **aipsi**

IMPLEMENTED BY **malabo** *ICT Advisory*

January 2024

Summary

1. THE OAD INITIATIVE

The Italian acronym OAD, Osservatorio Attacchi Digitali in Italia, indicates the annual survey of the digital attacks on IT systems, and their security measures, in Italy, provided by AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (https://www.aipsi.org/), Italian Chapter of the world-wide no profit ISSA (Information System Security Association, https://www.issa.org/).

The OAD survey started in 2008 with the acronym OAI, Osservatorio Attacchi Informatici in Italia, changed in OAD in 2016. With the 2024 edition, this initiative covers seventeen years of consecutive survey, since 2007 to 2023

Operationally OAD/OAI has been always implemented by **Malabo Srl** (www.malaboadvisoring.it), and in the last years is **a key initiative** of AIPSI, that sets up, guides, supports all the OAD initiative, and publishes the OAD final report, **ensuring its quality and independence** (also from the Sponsors).

OAD is the only initiative in Italy carried out with a strictly anonymous survey addressed to all companies, of every product sector and size, and to Public Administrations, via an online web questionnaire with pre-set answers that can be filled out with any modern browser.
The questionnaire is typically addressed to IT Systems Managers (CIOs), System Administrators, IT Security Managers (CISOs), Third Parties who manage the digital security of their customers, and for small and very small organizations, the top managers (CEOs) and/or owners which decide strategies, budget and plans for their information system and their cyber security.
The OAD main objective is to analyze and spread as much as possible the actual reality of cybersecurity and of intentional digital attacks on the information systems of companies and public bodies in Italy, as well as the security measures in place. The OAD questionnaire is anonymous, independent, authoritative and freely accessible by any person who operates and/or decides in the field of digital security.
The availability of correct and updated information on cybersecurity and digital attacks "local to Italy" is fundamental for the growth of knowledge and culture on these topics and for a concrete help, especially for small organizations, in the assessment of digital risks and in the choice of the most suitable prevention and protection security measures.
The OAD contributes to the awareness and knowledge of digital security for all users and decision makers of information systems, which is one of the objectives of AIPSI and ISSA (see https://www.issa.org/about-issa/ and https://www.aipsi.org/associazione/perche-aipsi.html): these knowledge and awareness are still low in Italy, as also highlighted by the indices of the European DESI survey (see https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts). Due to its importance in terms of communication, awareness and training on cybersecurity, OAD is part of the Italian national strategic initiative Digital Republic[1], as highlighted in https://repubblicadigitale.associazione.gov.it/it/i-progetti/.

Twelve OAD/OAI annual reports have been published (their covers in fig. 1): these reports cover the sixteen consecutive years of online surveys carried out to date, from 2007 to 2022.
The most recent OAD reports have an "executive summary" in Italian and English.
All OAI/OAD reports can be downloaded free of charge from the specific web site created for this initiative, https://www.oadweb.it/. A part of this site, although smaller than the Italian one, is in English:

---

[1] National strategic initiative promoted by the Italian Department for Digital Transformation of the Presidency of the Council of Ministers within the framework of the "Italy 2025" strategy: it aims to combat the cultural digital divide in the Italian population, to support maximum digital inclusion and encourage education on future technologies, accompanying the country's digital transformation process.

https://www.oadweb.it/en/. This site archives all the documentation (in some cases also video streaming) of the various events organized by AIPSI or in which it participated, to present and comment the OAD data.

As highlighted in fig. 1, on the covers of each report, since 2012, there are the logos of the Sponsors and the presentation sheet of each Sponsor is included as an attachment within the report (Attachment C, see §2.1).
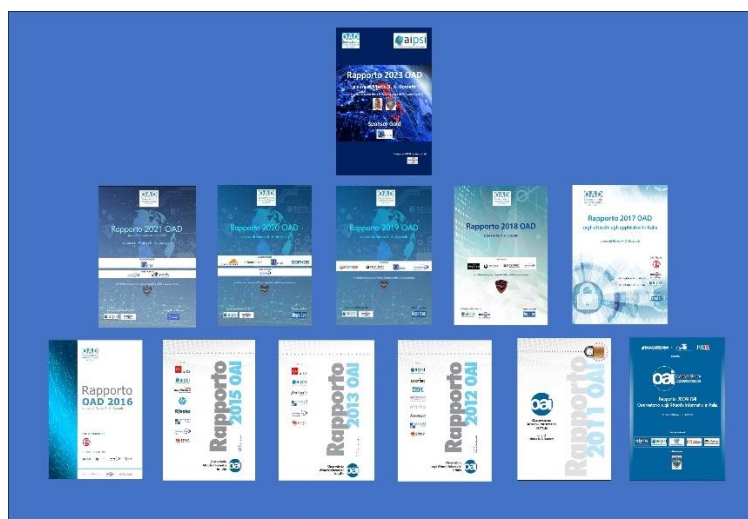

Fig. 1 The covers of the published OAD-OAI reports

Potential respondents to the OAD questionnaire are informed of the 2024 OAD survey and invited to fill in it through the various communication channels (websites, events, social networks, e-mails, articles and banners, etc.) of AIPSI, of the patronizing associations and of the Sponsors.
In previous editions, the number of potential respondents contacted could be estimated at around 5,000 people, mostly belonging to private companies, professional firms and, to a lesser extent, Public Administrations.

The number of reports downloaded from the OAD site or distributed via email, file transfer, file sharing, etc. have gradually grown over the years, reaching in the last three years a number per edition estimated at between 1000 and 1500. This figure is only an estimate, which includes not only the precise number of downloads made from the oadweb.it site, but also the estimated direct forwarding of the Final Report to many of the interested interlocutors by Sponsors, by Patrons and by those who had already downloaded it.

2. OAD 2024

The 2024 OAD survey will have a reduced and simplified questionnaire so as to reduce the time needed to complete it, while maintaining significant content for the analysis of the phenomenon of intentional digital attacks in the business sector and ensuring continuity with the main information collected in the previous editions.
For these reasons the online questionnaire, strictly anonymous, of OAD 2024:
- will contain only two questions on the attacks detected in 2023 in reference to the types of attacks and to the groups of attack techniques (see §2.1.1), so as to be able to have general trend data on the attacks (what is attacked and with which techniques) from 2007 to 2023;

- the in-depth questions will only concern the attacks suffered in 2023 on web environments and maybe on attacks on OT, Operational Technology, option still under discussion in AIPSI;
- questions on the digital security measures present in the information systems will be optional.

The questions on the suffered attacks are mandatory for all respondents: for those who have not detected attacks, the related questions are automatically skipped by the survey application, based on Limesurvey software.

There are also mandatory all the questions related to the type of respondent company/entity, to the most feared future attacks and to the role of the questionnaire compiler.

Upon completion of the entire questionnaire, <u>including the optional part on the security measures in place</u>, a qualitative **macro evaluation of the security level** is automatically provided: a level that emerges from the answers provided, and that depends, in general, from the type of company and from its needs for digital security. This macro-assessment is of particular interest especially for small and very small organizations.

As in previous years, AIPSI will establish patronage with associations of the various product sectors (as well of the local and central public administrations), and of specific professions (for example lawyers, notaries, accountants, doctors, CIOs, CISOs, DPOs, etc.).

AIPSI will try to expand the number of media used, and to obtain a more incisive involvement of newspapers to raise awareness of the 2024 OAD survey and of its final report, and, first of all, to promote the compilation of the questionnaire .

AIPSI will hold specific events with some of the patronizing associations, and if the number of respondents per product sector allows it (>100), to carry out specific analyzes for these sectors.

Please note that AIPSI **cannot guarantee** complete coverage of the various product sectors, and even less can it guarantee the effective and active collaboration of the patronizing Associations. The campaign that will be undertaken by AIPSI with all these interlocutors, and the reduction in the number of questions in the online questionnaire, should lead to an increase in the total number of respondents: but it is not possible to guarantee the Sponsor a predetermined extension of the pool of respondents (and then of readers of the Final Report) for the various sectors.

2.1. The questionnaire OAD 2024

As already indicated in the previous paragraph, the 2024 questionnaire will be focus on the intentional attacks detected in 2023 on web sites and applications. AIPSI is evaluating whether to include a set of questions for attacks on the world of OT, Operational Technology.

OAD 2024 will use a strictly anonymous online questionnaire, substantially structured into two main parts: the attacks detected in 2023, and the digital security measures in place. The answers related to the attacks will be mandatory, while these on existing security measures will be optional, but required to have the macro evaluation of the security level.

If no attacks have been detected, the online questionnaire system automatically skips the related questions and moves on to the next ones.

2.1.1 The questions on the detected attacks

The two general and mandatory questions, necessary to guarantee continuity with those of the previous sixteen years on the spread of intentional digital attacks in Italy, concern:
- the types/families of attack that refer to <u>what is attacked</u>:
  - o Physical destruction of ICT devices or their parts
  - o Theft of mobile user devices (smartphones, tablets, etc.)
  - o Theft of fixed ICT devices or their parts (PCs, servers, storage systems, etc.)

- o Theft of information from fixed ICT systems
- o Theft of information from mobile user systems
- o Attacks on the identification, authentication and authorizations of the users
- o Attacks on networks, local and geographic, fixed and wireless, and on DNS
- o Attacks on individual ICT systems as a whole (from user devices to storage servers and cloud services)
- o Attacks for unauthorized modifications to application programs and their configurations
- o Attacks for unauthorized modifications to the information processed by ICT systems
- o Deniel of Services/Distributed DoS attacks (DoS/DDoS)
- o Attacks on the parts of our IT system outsourced in cloud or in housing/hosting services
- o Attacks on the OT, Operational Technology, systems of your IT system (Internet of Things, industrial automation and robotics, etc.).
- the families of attack techniques, which refer to <u>the attack's modes</u> in terms of which technical techniques were used:
  - o Physical attack
  - o Malicious and unauthorized collection of information
  - o Malicious scripts and programs
  - o Autonomous agents
  - o Toolkits
  - o Botnets and similar
  - o Use of Artificial Intelligence tools
  - o Use of two or more attack techniques, including APTs, Advanced Persistent Threats.

Detailed questions about detected attacks on web, and may be on OT, will include:
- whether the systems attacked are on premise, outsourced in hosting or in the cloud, or in a mix between outsourcing and on premise;
- the probable attack techniques used (listed above) and, in greater detail for web environments, which vulnerabilities were probably exploited by referring to the OWASP top 10 in the case of the most serious attack suffered;
- the most serious technical and economic impacts experienced by the most serious attack;
- the possible reasons for the most serious attack;
- the maximum time to recover after suffering the most serious attack.

2.1.2 The digital security measures in place

As previously indicated, all these questions will be optional. However, it would be advisable to be compiled, so as to obtain:
- a checklist of digital, technical and organizational security measures that could or should be implemented on the information systems of the respondent;
- a macro qualitative analysis of the existing security level, based on the answers provided, with the list, among these answers, of those that highlight the most serious shortcomings. In practice, a first indication of the main improvements in digital security that should be made.

As in the questionnaires of recent years, the survey of digital security measures in place will refer to the following measures:
- **Technical measures**
  - o Digital security architecture, integrated with the IT system architecture, which may include Zero Trust, SASE, SOAR, etc.

aipsi

- o Physical countermeasures
- o Identification, Authentication, Authorization (IAA)
- o Local and geographic networks' countermeasures
- o Logical protection of each ICT system (as a whole)
- o Application protection
- o Data protection
- **Organizational measures**
  - o Digital security structures, roles, skills, certifications
  - o Digital security policies and procedures
  - o Digital security contracts and clauses with Third Parties
  - o Awareness of digital security at all levels of the organizational structure
  - o Auditing
- **Management and governance measures**
  - o Digital security control and monitoring (operational management)
  - o Strategic governance
  - o Disaster Recovery.

Further questions in the questionnaire will concern:
- type and macro characteristics of the respondent's company/entity: product sector, number of employees, organizational structure for cybersecurity and primary needs for security measures for its activities (this question is asked at the beginning of the survey)
- How attacks were detected and managed when they occur
- types of attacks most feared in the near future.
- role of the questionnaire compiler.

2.2 OAD 2024 Report

The final report will be published and made available free of charge to all interested parties on the OAD and AIPSI websites, within the expected timeframes indicated in §5.

The Report will initially have an Executive Summary in Italian and English.

A specific chapter will be dedicated to the data provided by the Postal and Telecommunications Police, relating to the whole 2023. These data will concern, as in previous years, digital attacks on Italian critical infrastructures, digital attacks on the world of banking and finance, digital terrorism .

The final report will also include the following attachments:
- Annex A - Methodological aspects of the 2024 OAD survey
- Annex B - Glossary of the main terms and acronyms on cyber attacks
- Annex C - Sponsor Profiles (an "institutional" sheet for each Sponsor, of 1, 2 or 3 pages in A4 format depending on the type of sponsorship, see §8)
- Attachment D - Sponsor Profiles (logo, website URL, 3-4 lines of description)
- Annex E - References and sources
- Annex F - Profile of the Author(s) of the 2024 OAD Report
- Attachments G, H - Profiles of AIPSI and Malabo Srl

The 2024 OAD Report, as soon as it is available (see §6), will be downloadable free of charge from the OAD website and from the AIPSI website.

As an example of a final report, and its summary, see the OAD 2023 Report:
https://www.aipsi.org/eventi/eventi-in-programma/902-aipsi-ha-pubblicato-il-rapporto-oad-2023-ora-scaricabile.html

All previous OAD/OAI reports are archived, and downloadable, year by year from
https://www.oadweb.it/it/rapporti-e-relativi-convegni.html

3. TO THANK THE RESPONDENTS TO THE 2024 OAD QUESTIONNAIRE

Who will complete the 2023 OAD Questionnaire will be able to download for free two issues of the ISSA Journal magazine, reserved for AIPSI-ISSA Members.
The decision of which numbers to use of the ISSA Journal is currently underway, in order to select the two numbers with the topics of greatest interest to the Italian respondents.

4. OAD 2024 SCHEDULING

The overall framework of the activities planned for OAD 2024 is divided, month by month, into the following activities:

- **JANUARY 2024**
    - o Setting up of the OAD 2024 initiative within the AIPSI Steering Committee
    - o Drafting sponsorship and patronage proposals and sending them to the potential interested companies and associations

- **FEBRUARY 2024**
    - o Design and installation-activation of the online questionnaire
    - o Start of promotional campaign for questionnaire's compilation
    - o Contacts for patronages and sponsorships

- **MARCH - JUNE 2024**
    - o Campaign for questionnaire's compilation
    - o Contacts for patronage and sponsorships

- **MAY-JUNE 2024**
    - o The online questionnaire system will be closed, depending on whether and when the minimum number of respondents (necessary for an anonymous web survey) will be reached.
        - ▪ If not reached, AIPSI will carry out a further specific promotion for the compilation of questionnaires person by person, in particular with reference to CIOs and CISOs
    - o Start the analysis and the data processing of all the information collected by respondents. Otherwise AIPSI will, in collaboration with the Patrons and Sponsors, a specific promotion.

- **JUNE-JULY 2024**
    - o Processing of data collected from online questionnaires
    - o Drafting of the 2024 OAD Report and its publication
    - o Promotional campaign for the download of the 2024 OAD Report
    - o AIPSI "hybrid" event (physical and remote meeting in audio video conference) for the official presentation of the 2024 OAD Report with a round table to discuss the the survey results with the representatives of the Gold and Diamond Sponsors (this event could be moved to September).

- **AGOST-SEPTEMBER 2024**
    - o Drafting of notes and articles in the various media relating to the 2024 OAD Report
    - o First webinars for Gold and Diamond Sponsors

- **SEPTEMBER-DECEMBER 2024**
    - o Periodic provision to Sponsors of download data for the 2024 OAD Report
    - o AIPSI presentations, in various events, of some results from the 2024 OAD survey.

5. WHY IT IS WORTH SPONSORING OAD 2024

The sponsorship of OAD 2024 allows any company/institutions, in particular ICT and cyber security companies, to obtain important and qualified visibility of their brand and of their products/services, thanks to the Sponsor sheets published in the Annex C of the Report (see §2.2), their logo on the cover and in the numerous presentations of the OAD results in the AIPSI various events and webinars. Visibility accentuated by an immediate "time to market" with those who have a negative assessment of the digital security level, and have immediately the references of the sponsoring companies which can help in the hardening the digital security level of the information system.

The sponsorship contributes also actively to support the only Italian online survey via web on digital security and make Sponsor company and their brands known to the thousands of AIPSI interlocutors who read the reports and articles on OAD, and who participate in the various events of the association: all potential customers of the Sponsors.
The AIPSI events help the diffusion of the OAD data and, above all, their circulation in the qualified business communities of decision makers and "ICT influencers". All this allows Sponsors to obtain large visibility.

6. OAD 2024 SPONSORSHIP

AIPSI allows the following types of sponsorships:

1. **<u>Silver</u>** Sponsorship, the basic one with a prize of **€ 2.000,00 + VAT**, which entitles to:

a) the Sponsor logo on the online questionnaire and on the cover of the 2024 OAD Report;
b) one A4 page presentation of the Sponsor in the Annex C of the 2024 Report (see §2.2), with institutional information and an highlights of his products/services for the digital security;
c) the availability of the figures and graphs in high definition of the 2024 Report for any publications (blogs, websites, social networks, on paper, etc.) by the Sponsor, with the AIPSI obligation to always show, for each published figure, the brand ©OAD 2024 (already present in the figures and graphs provided, and not to be deleted);
d) the visibility of the Sponsor's logo in all the AIPSI presentations on OAD;
e) the Sponsor's logo on the OAD and AIPSI web pages to download the OAD 2024 Report; the promotion of the 2024 survey and of the final report on social networks and other media in which OAD, AIPSI, Malabo and the various Patrons and Sponsors are active.

A single invoice of €2,000.00 + VAT is issued to the Silver Sponsor by AIPSI upon receipt of the order; payment must be made within 30 days of the invoice date.

2. **Gold Sponsorship**, with a prize of **€ 5.000,00 +VAT.** In addition and/or in modification to what is provided for the Silver one, it entitles to:
    a) a larger size of the Sponsor logo on the cover of the Report and on the AIPSI and OAD websites as Gold Sponsor;
    a. two A4 pages in its presentation in Annex C of the OAD 2024 Report;
    b. the inclusion of the logo and the link to the Diamond Sponsor website on the home page of the AIPSI website under the heading "Sponsor AIPSI 2024";
    b) the participation of a representative of the Sponsor at the Round Table of the (hybrid) webinar that will present the OAD 2024 Report.

Payment can take place in a single tranche or in two. Two invoices can be issued to the Gold Sponsor by AIPSI, the first of €3,000.00 + VAT upon receipt of the order, the second of €2,000.00 + VAT upon publication of the Final Report. Payment must be made within 30 days of the invoice date.

3. **Diamond**, with a prize of **€ 10.000,00 +IVA.** In addition and/or in modification to what is provided for the Gold one, it entitles to:
    a. an even larger size of the Sponsor's logo on the cover of the 2924 Report and on the AIPSI and OAD websites as Diamond Sponsor;
    b. three A4 pages in its presentation in Annex C of the OAD 2024 Report;
    c. the possibility of participating and collaborating in defining the questions and answers in the 2023 OAD questionnaire, if registration takes place by 15/02/2024;
    d. the possibility for a top manager of the Diamond Sponsor to participate in the AIPSI Board of Directors, suggesting/proposing specific initiatives;
    e. a specific AIPSI-Sponsor event/webinar, which content will be agreed and in any way will include some of the results of the 2024 survey, that are significant for the Sponsor. The webinar may use the AIPSI platform or the one provided by the Sponsor itself;

f. the creation of a specific article, in collaboration with some AIPSI leader, that will be published in one or more magazines, chosen from those of the AIPSI and/or used by the Sponsor; this article will be published also on the AIPSI and OAD websites.

Payment can take place in a single tranche or in two. Two invoices can be issued to the Diamond Sponsor by AIPSI, the first of €6,000.00 + VAT upon receipt of the order, the second of €4,000.00 + VAT upon publication of the Final Report. Payment must be made within 30 days of the invoice date.

7. THE INTELLECTUAL PROPERTY OF OAD 2024

The intellectual property and copyrights of the entire initiative OAD 2024, including the online questionnaire and the contents, figures and graphs of the OAD 2024 Report, belong, as for the previous editions, to AIPSI and Malabo Srl which allow their use to Sponsors, with the obligation to cite the source on the figures and graphs of the Report using the brand **©OAD 2024**.

8. HOW TO JOIN THE SPONSORSHIP OF OAD 2024

To join the sponsorship of OAD 2024, simply complete all the entries in the membership form on page 12, sign it by the person with signing powers, scan it and send the signed and scanned form by email as an attachment to aipsi@gigapec.it. After receiving the form, the applicant Sponsor will be contacted by telephone/e-mail, and the related invoice will then be issued by AIPSI.

8.1 Time frame available to sign up for the sponsorship

The time frame for signing this offer goes from January 2024 to June 2024, but practically it has the limit of **2-3 weeks before the 2024 Report will be published**, so that the Sponsor's presentation sheet can be edited and inserted in the Attachment C, and its logo on the cover of the Report.

It is important to highlight that the sooner the Sponsor will confirm its sponsorship, the longer its logo and link will be visible and followed by visitors to the websites, social networks, events that will promote OAD 2024.

OAD 2024 SPONSORSHIP FORM

This form, completed and signed, has to be sent in e-mail to aipsi@gigapec.it

Our Company confirms to AIPSI its sponsorship of OAD 2024 with the choice selected below, that implies the related rights and conditions detailed in this proposal
(Please, place a cross in the chosen box)

☐   Silver Sponsorship   € 2.000,00 + VAT
☐   Gold Sponsorship   € 5.000,00 + VAT
☐   Diamond Sponsorship   € 10.000,00 + VAT

Company: ....

Address: ....

City: ....   **Postal Code**: ....

VAT: ....

Company E-mail (possibly REM for Europe)**:** ....

We will issue a purchase order to AIPSI: *NO/YES*   ORDER NUMBER: ....

Operational contact person

First Name: ....   **Last Name:** ....

Phone: .... **Mobile**: ....**E-mail:** ....

Responsible/Manager with signing power

First Name: ....   **Last Name:** ....

Business role: ....

Phone: .... **Mobile**: ....**E-mail:** ....

Responsible/Manager signature: ....

Place : ……………………………………… ***Date***: ……………………………………

AIPSI
www.aipsi.org
Registered office: Via Savona 26 - 20144 Milano
Tel: +39 02 72191512
E-mail: aipsi@aipsi.org
VAT : 05311540966

MALABO S.r.l.
www.malaboadvisoring.it/en
Registered office: Via del Caravaggio 14 20144 Milano
Tel: +39 02 72191512
E-mail: info@malaboadvisoring.it