Inside

INTELLIGENCE & SECURITY INVESTIGATIONS

InsideForensics

www.inside.agency • info@inside.agency

Your new choice for risk management

ABOUT US

INSIDE gathers information, at a national and international level, that is useful to companies for risk management, in compliance with regulations, professional ethics and corporate governance standards. The information is used to assess the economic, financial and reputational risks of organisations and individuals with whom the company may establish business relations.

This series of information allows **strategies and techniques to be prepared to counteract the dangers** inherent in various market sectors (pharmaceuticals, automobiles, insurance, finance, government...), which can affect small businesses as well as larger companies.

Reports can also be prepared on **politically exposed persons** (PEPs), who hold or have previously held public office, and are therefore more exposed to the risk of committing certain crimes, such as corruption, bribery or money laundering.

INSIDE **helps organisations to know their business partners**, guiding their activity towards more informed decisions, through a range of services that ensure regulatory compliance and fulfilment of legal and auditing requirements (regulations of the Foreign Corrupt Practices Act - FCPA, the UK Bribery Act, Anti-Money Laundering – AML controls, the USA PARTRIOT Act and Countering the Financing of Terrorism – CFT controls); the research conducted - which can cover all market sectors and any organisation, regardless of its size - provides a thorough check on potential business relations, highlighting any risks of corruption arising from a geopolitical analysis of the case.

The reports provide all information on a company and its directors, activities, history, administration, conflicts of interest, financial liabilities, legal and judicial affairs (compliance risk), and reputational risk. They also include verification of statements by the administrators, compliance with anti-money laundering (AML) rules, anti-corruption controls, FCPA and UKBA rules, sanctions against Iran, and International and US due diligence procedures.

INSIDE reports are generally recommended for verification of financial crimes, but are not limited to this: the research by INSIDE provides **a valid solution in situations of geopolitical risk** (high-risk countries) regarding a transaction or an individual involved in it, for supply chain and due diligence checks, before major investments such as mergers or acquisitions, and for **an integrated compliance programme**.

INSIDE conducts the investigations itself, thereby maintaining a high level of quality and efficiency, with access to a large number of **operators located across five continents and speaking over 60 international languages**; it also uses native speaker professionals, who can grasp language nuances that are often incomprehensible to those outside of a particular culture. The information and “open source” data collected is abundant and of high quality, as the various sources used are constantly updated with foreign official information.

INSIDE offers professional IT and technology services, skilfully combining considerable advanced business skills with proven experience in the recruitment and training of its specialists.

To provide the best possible support to its Clients (companies and lawyers, as well as private individuals who feel the need to monitor their children more closely), INSIDE **has brought together the best expertise in the field of security** in a special ranges of services known as IT Security.

The Service Line operates throughout Italy; the area of intervention of the INSIDE Forensics Division is described below:

Forensic Analysis and Incident Management (FOR-SEC): INSIDE's intervention in this area is normally in response to errors, accidents, intrusions or legal action. The advice provided covers forensic analysis of digital media, secure deletion of data, the recovery of data from damaged digital storage media and the definition and implementation of technological processes and procedures for proper incident management. The staff that operate in this field hold GCFA and GCIH certification (SANS certifications) and **follow the guidelines laid down by the US Department of Justice** for the seizure and preservation of digital crime evidence.

Interventions can be carried out on a series of devices:

- computers and storage devices - Computer Forensics;
- electronic devices that use mobile technology - Mobile Forensics: mobile phones, smartphones, tablets and SIM cards, of any make and model;
- "closed" equipment - Embedded Forensics: game consoles, skimmers used for the cloning of credit cards, PDAs, organisers, Mp3 players, databanks and closed circuit systems;
- Internet - Network Forensics: e-mail; social networks (Facebook, Linkedin, Twitter, MySpace...), data exchange systems (FTP, Peer to Peer...), VoIP (Skype is the best known), Virtual Private Networks (VPN);
- software - Software Forensics: software illicitly possessed and marketed with a significant economic return for the perpetrator; encryption software, pirated video games; software designed to bypass security systems (password cracking).

The Service Line not only manages INSIDE's own expertise, but also provides for the continuous training of its consultants and clients, with specific events ranging from seminars to safety courses organised internally or externally. The Service Line also includes SANS instructors who can **give specialised courses with certification** accredited under standard ISO 17024, such as perimeter security, incident management and web application security.

INSIDE considers it essential for the staff of the Service Line to be part of the development and innovation in the field of ICT Security, with active participation on the boards of SANS, OWASP and OSSTMM, as well as internal development projects ranging from advanced forensic analysis of digital signals to the definition of analytical systems for digital fraud prevention (pre-crime).

Description and Mode of Delivery of the Service

INSIDE provides its Clients with its own expertise in the field of IT security, and is committed to the providing specific consultancy through its own IT Consultants for the execution of the following forensic analysis activities, with provision of documentation:

- Forensic analysis of the content of the Client's phone to detect any malicious software directing calls to unauthorised numbers or at higher rates;
- Data recovery from digital media (deleted data and/or hidden data) on devices owned by the Client and transfer of the data to an external device (USB - CD ROM).

The analysis of the information extracted from the device will be based on keywords provided by the Client (names, addresses, phone numbers, etc.) and the consultant's experience in responding to any questions raised by the Client. Please note that the Client is required to provide all necessary information to ensure access to the device to be analysed (e.g. passwords, PIN numbers, etc.). If these are not known, INSIDE will apply analysis and/or acquisition methods that may not, however, be exhaustive or complete.

1. DATA RECOVERY INTERVENTION METHODOLOGY

INSIDE's Forensics Division is able to handle all data losses caused by human error, sabotage or events of various kinds.

During the data recovery process, the IT personnel work on the broken or malfunctioning device or disk with the aim of **temporarily restoring its functionality and extracting the data**. The extracted information is then reconstructed and saved in a format accessible to the user.

- **Prognosis**: once they receive the damaged data storage media, the IT Consultants of the INSIDE Forensics Division begin the prognosis (technical analysis) phase to identify the problem and understand which files can be recovered. When this analysis is completed, the Client is provided with a list of recoverable files, including a description of the state of integrity of each one.
- **Data Recovery**: once the restoration of the recoverable files has been authorised, the data recovery phase begins, after which the files are stored on the Client's external backup media.
- **Data Restitution**: the backup media with the recovered data is sent to the Client by express courier. To ensure greater security, the data is encrypted and the password is sent by e-mail.

2. FORENSIC ANALYSIS INTERVENTION METHODOLOGY

We describe below the sequence used by the INSIDE Forensics Division for carrying out data analysis activities, from the assignment of the task to the final report:

- **Identification**: to begin with, all potential sources of data that can provide valid evidence presentable in court are identified and an appropriate work plan is devised.
- **Acquisition**: digital data should never be accessed without proper tools and procedures, due to the risk of invalidation or inadmissibility of the evidence presented in court. Digital information is fragile and can easily and/or inadvertently be altered by unqualified persons, even merely by switching on the device on which is stored. The intervention methodology used by the INSIDE Forensics Division ensures that the data is acquired without any alteration and/or damage. A duplicate forensic copy of the data is made and its integrity is checked using hash functions. All the operations are adequately documented to ensure a proper chain of custody.
- **Extraction**: INSIDE works on the forensic copy acquired to extract the data and information contained in this perfect copy of the storage medium under analysis. Our extraction process ensures the recovery of deleted files, hidden files, temporary files, file fragments and other information stored on various devices such as personal computers, servers, mobile phones, smart phones and navigation systems.
- **Data analysis**: once the information has been extracted, it is analysed to reconstruct the activities carried out with the digital device. A final report is then prepared containing all relevant information, which can be used for internal appraisals within the company or in court.

3. TOOLS USED

The INSIDE Forensics Division uses the best professional equipment available.

Forensic copies are made using professional equipment that is certified and accredited for legal use.

The tools we mainly use include the following:

- **LOGICUBE FORENSIC FALCON**: for making forensic copies of hard disks;
- **UFED**: for the extraction and analysis of data from mobile devices;
- **CAINE and SLEUTH KIT - AUTOPSY**: for analysis of the data;
- Other tools similarly recognised and established in the field of forensics.

The exclusive use of software tools alone, however, is not sufficient to obtain a satisfactory result, which also requires the significant **experience and knowledge** of the staff assigned by INSIDE to use them. For this reason, careful and thorough manual checks are also carried out to assess the vulnerabilities found and detect any further security breaches.

4. DOCUMENTATION DELIVERED TO THE CLIENT

On completion of the analysis activities, the Client is provided with **two separate documents** containing the information recovered from the devices that were analysed, and the complete analysis procedure that was performed, to ensure the repeatability of the analysis.

The documentation is provided on standard INSIDE document forms, or on templates provided by the Client, without prejudice to the possibility of the structure being modified by INSIDE staff to provide the most complete documentation possible of the analysed material.

5. SERVICE PROVISION LOCATIONS

The activities described above shall be carried out in the forensics laboratory at the INSIDE headquarters, according to the work plan agreed with the technical manager assigned by the Client.

The activities shall be carried out using laptop computers owned by INSIDE, on which all of the tools used shall be **installed and duly licensed**. These computers shall also have updated antivirus programs and personal firewalls.

6. DELIVERY TIMES

The activities shall be completed within 15-20 working days (unless scheduled otherwise).

This time schedule may be changed based on decisions taken while the activities are in progress and ratified during project progress meetings.

7. CONTROL STRUCTURE

The activities of the INSIDE Cyber Security Division technicians are supervised by a **Service Line Manager** who is exclusively responsible for the activities, has sole authority to receive all formal communications from the Client and is delegated to participate in the project control phases.

Inside
INTELLIGENCE & SECURITY INVESTIGATIONS

www.inside.agency • info@inside.agency

MAIN OFFICE

SWITZERLAND
Via Maggio, 1/C
6900 Lugano
T +41 (0)91 260 16 42
F +41 (0)91 228 03 95

OFFICES AROUND

UNITED KINGDOM
Crown House, 72 Hammersmith Rd
Hammersmith, London, W14 8TH
T +44 (0)20 75 59 13 11
F +44 (0)20 35 14 68 50

USA
6800 Jericho Turnpike, Suite 120W
Syosset, New York, 11791
T +1 (0)516 393 58 52
F +1 (0)516 393 58 19

RUSSIA
31st floor, stroenie 1, bld. 3,
Begovaya str, Moscow, 125284
T +7 (0)499 277 13 03
F +7 (0)499 287 66 00

ITALY
Via Monte di Pietà, 21
20121 Milano
T +39 (0)2 86 33 73 42
F +39 (0)2 94 75 26 15

ITALY
Via Ludovisi, 35
00187 Roma
T +39 (0)6 42 03 73 97
F +39 (0)6 94 80 17 11

UNITED ARAB EMIRATES
Building 3, Plot 598-676, Dubai Investment
Park, Green Community, DUBAI, 212880, EAU
T +971 (0)4 80 19 276
F +971 (0)4 80 19 101

HONG KONG
25 Westlands Road, Quarry Bay Berkshire
House, Unit 2402-07, 24th HONG KONG
T +852 (0)28 24 85 28
F +852 (0)37 19 81 11

SOUTH AFRICA
First Floor, Willowbridge Centre, 39
Carl Cronje Dr, Cape Town, 7530
T +27 (0)21 974 6276
F +27 (0)21 974 6101

BRAZIL
Top Center Paulista, Paulista Avenue, 854
Bela Vista – 10° floor, São Paulo, 01310-913, Brasile
T +55 (0)11 21 86 04 42
F +55 (0)11 21 86 02 99