



WHAT IS FORENSIC TECHNOLOGY?

Effectively using technology to uncover and manage evidence and intelligence in contentious legal and regulatory situations.

WE SEPARATE FORENSIC TECHNOLOGY INTO FIVE DIFFERENT CATEGORIES:



Applied data analytics



Cybersecurity



Digital investigations



Electronic discovery and disclosure management



Information governance

GLOBAL TRENDS INFLUENCING THE USE OF FORENSIC TECHNOLOGY



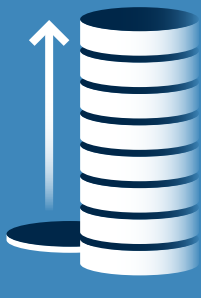
REGULATIONS & GOVERNANCE

Extensive data handling policies (e.g., GDPR) and investigative teams assisting with compliance.

THE EVOLUTION OF BIG DATA

The amount of data being generated and its utilisation in organisations.

Experts predict a **4300% leap** in the annual production of data by 2020.



PROTECTION

Data management and protection against insider threats and cyber-attacks.

BYOD

Since the advent of smartphones and tablets, workplaces have been adopting and evolving toward Bring Your Own Device (BYOD) policies.



59% of organisations allow employees to use their own devices for work purposes.

THE NEED FOR FORENSIC TECHNOLOGY: KEY THREATS BY REGION

UNITED KINGDOM

A wide range of systems, devices and apps used to communicate and extract data from organisations.



30,000 out of 40,000 devices annually linked to forensic threats are mobile phones.

UNITED STATES OF AMERICA

A workforce sufficiently trained in key processes is imperative for proactively managing cyber defenses.

Security teams currently face **244 new cyberthreats every minute**.



GERMANY

Data disclosure is relatively new legal territory. As companies expand and trade more globally, their exposure to foreign discovery requests will significantly increase.

German trade with the U.S. and U.K. defined by goods imported and exported, increased by **26%** and **43%** respectively from 2006 to 2016.



RUSSIA

Regulations relating to data localisation and data transfer.



The recording, systematisation, accumulation, storage, updating (renewal, amending) and extraction of personal data of Russian citizens can be done only through databases located in Russia.

UNITED ARAB EMIRATES

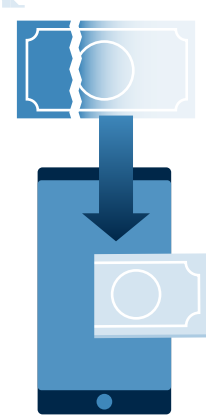
Lack of data control due to significant task delegation to technical staff.



More than **40%** of organisations do not know where their data is stored.

INDIA

Increased payment data and platform vulnerabilities resulting from increased growth in digital payments thanks to governmental de-monetisation initiatives.



68% of the nation's hard currency has been taken out of circulation and **online payments** have surged **250%**.

One in every 10 transactions is now rejected on suspicion of fraud.

CHINA/HONG KONG

Localised cloud and social media platforms like WeChat are used simultaneously with business systems, and many companies still prefer hard records to electronic data.

China is at **65 / 100** on BBVA Digitalization Index*

KEY OPPORTUNITIES IN FORENSIC TECHNOLOGY



GDPR and other regulatory changes are an opportunity to audit, review and organise your company data, creating a clean house for the information you store.



Sufficient training of people in processes is key to being proactive and managing cyber defenses.

An investment in user awareness and training effectively changes behavior and reduces security-related risks by **45% to 70%**.



Involve C-suite stakeholders in data infrastructure and process architecture.

71% of C-Suite leaders are not engaged in cybersecurity prevention.



Government initiatives and the rise of cloud computing offer potential benefits for all types of organisations.

In India, the estimated growth of public cloud market is pegged at **\$7.4-7.6 billion** and private cloud at the rate of **\$7 billion by 2020**.

By 2020, the aggregate market size of China's cloud computing industry is expected to hit 686.6 billion yuan (about **\$103.6 billion**).

DON'T SIMPLY REACT. PROTECT.

Data is the lifeblood of an organisation. Knowing its depth, usage and level of security should be a top priority for business leaders.

THE RISKS ASSOCIATED WITH LACK OF PROACTIVITY:



Regulatory and compliance violations and penalties



Subsequent costs and ramifications of security breaches



Employee misuse of proprietary information and consequent damages

PROACTIVELY MANAGE YOUR FIRM'S DATA AND INTELLIGENCE. PLAN YOUR FORENSIC TECHNOLOGY STRATEGY TODAY.

alvarezandmarsal.com/expertise/forensic-technology