

“Tackling Fraud” - How Sapphire Helped the SFO Bring Cases Through the Courts

The Serious Fraud Office (SFO) is a government department responsible for investigating the most complex and largest fraud cases in the jurisdiction of England, Wales and Northern Ireland. It also brings prosecutions in the Crown Courts. As both investigator and prosecutor in the most difficult cases of their kind, the SFO has to be at the front edge of fighting economic crime.

In carrying out these investigations, the SFO is faced with an ongoing challenge. The organisation is required to examine and analyse data held on, or retrieved from, computer storage media for the purpose of presentation in court.

The SFO needs to react quickly to these urgent demands and at times needs to seek assistance from other organisations with the requisite skills to carry out the necessary analytical work. Aware of this issue, it frequently invests in the time and resources of an expert third-party security consultancy. In Summer 2007 as part of this programme SFO appointed leading information security advisor, Sapphire to provide computer forensic support.

As Keith Foggon, Head of the SFO's digital forensics unit, explained: “There were several factors behind the choice of Sapphire, with the key factors being firstly, in our view, its technical skills and in particular its ability to analyse digital material. Secondly, Sapphire demonstrated great flexibility; it was willing to change its working patterns completely to suit our own.

“Rather than taking forensic work into its Head Office laboratories in Stockton-on-Tees, it sent consultants out to work on-site at our London offices on a six-month assignment. We were impressed by Sapphire's willingness to move outside its ‘comfort zone’ in this way,” Foggon added.

Getting the Job Done

This initial project involved Sapphire helping the SFO to analyse hundreds of separate items of evidence relating to one particular fraud case. In addition to data analysis, the commission also involved some imaging and data extraction work.

Following its appointment by the SFO, Sapphire initially provided one consultant on site in London, expanding to four over time. Working to a tight timetable, Sapphire achieved or exceeded every metric set by the SFO in terms of prompt delivery of evidence.



Following the completion of this work, Sapphire was then given a further urgent project to complete. For this job, the SFO agreed to utilise Sapphire's laboratories.

It visited the facilities, assessed them and gave Sapphire the green light to receive evidence from the SFO, store it in a secure environment on-site and have work carried out on it in the imaging suite of the Stockton-on-Tees-based forensics laboratory.

John Morrison, Managing Director at Sapphire commented "This confidence in our work covers our range of technical services, our levels of service delivery, in particular our ability to deliver to tight deadlines, the skills of our individual staff and the security levels we could guarantee within our forensics lab and imaging suite."

"Our ability to maintain confidentiality within the building was also critical. The fact that we had achieved ISO 27000, the international standard for information security, gave the SFO full confidence that we would handle information on a strictly need-to-know basis," he added.

During one particular commission, Sapphire set up a secure portal for the SFO which enabled Sapphire to encrypt and then upload case notes concerning projects on which it was working. It also allowed the SFO to then download case notes and images to their own systems.

A Myriad Benefits

The key benefits of the relationship with Sapphire from the SFO's perspective is that it is working with a trusted partner, capable of providing meaningful and relevant data around current court cases in a timely manner. These excellent service levels enable the Digital Forensic Unit to meet its own deadlines for submission of evidence and even to deliver ahead of the tight schedule set for it by the case teams.

In addition, contracting work out to a third-party's premises allows the SFO to make more structured use of its own environment.

By adopting this approach, they can obtain a fixed cost upfront from Sapphire for the total project. If additional work has been required, Sapphire has been quick to alert the SFO to the extra costs involved.

Sapphire has also been exceedingly responsive in meeting tight project deadlines. Foggon confirmed: "It retains complete focus and control over jobs that are going out, it has pre-defined timescales for when work must be completed and this enables us to schedule our processes around it."



Assessing the Situation

In addition to the forensic projects, the SFO also appointed Sapphire to carry out extensive penetration testing of its digital forensics unit's local area network.

Sapphire was chosen for this project partly because of the technical expertise of its staff and partly because it met the rule that any company carrying out penetration testing at the SFO must be part of the Communications-Electronics Security Group (CESG) IT Health Check scheme, known as CHECK. Companies belonging to CHECK are measured against high standards set by CESG. CHECK Service Providers are currently permitted to work on systems processing protectively marked information up to, and including, CONFIDENTIAL.

The work involved carrying out the DFU's annual penetration test and an annual internal vulnerability assessment of the Unit's local area network. The objective was to ensure that the confidentiality and integrity of the network was maintained at all times, that there was no potential for information leaks, or for individuals to traverse networks. In short, the digital forensics unit had to be seen to be and validated as being, absolutely secure.

Looking to the Future

As with its forensics work, Sapphire once again was able to demonstrate total commitment to completing the penetration testing project efficiently.

As Foggon explained, "The beauty of working with a high-quality consultancy like Sapphire is the fact that it does not need to get involved in any of the day-to-day operational issues. It can concentrate purely on delivering the work to the highest standard possible."

"We have been consistently impressed by Sapphire. In addition, the case teams that we work with have made specific requests to use consultants from Sapphire because of their ability to work effectively and accurately," he added.

Looking to the future, the SFO Sapphire will certainly be considered for computer forensic support.

