

Forensics

What's the worst that could happen?



Statistics show that organisations are far more likely to suffer a serious information security incident from an insider rather than an external intruder. Those with access to sensitive and/or valuable information, given sufficient motivation, may be tempted to abuse their position. Funds may be gradually siphoned off into another account; valuable databases, sales leads, customer contacts, credit card information – the list goes on and on – may be stolen and sold to a third-party.

Theft of information can frequently remain undiscovered for a long time: the information, if simply copied, remains in its original place after all. Horror stories

abound indicating the worst that could happen. You only have to pick up a newspaper to read of some “white collar” crime resulting in loss of reputation, liquidation of organisations, etc.

Prevention is better than cure, and it makes sense to ensure that your information security measures are up to scratch. Whilst it is nigh impossible to protect 100% against an inside job, staff will know what the organisation’s attitude is toward the policing of corporate systems. They will know, or will hear rumours about, what type of crimes may have been successfully or unsuccessfully committed, and what action may have been taken against staff. An organisation showing that it has the

ability to catch and prosecute this type of insider attacker will dissuade them – much like the shop sign, “We always prosecute thieves.”

Forensics

Nevertheless, sometimes someone will step over the mark, or some disaster may occur. This is where forensics comes into play. The term “forensic”, though it might give rise to thoughts of dead bodies and DNA testing, simply means “suitable for use in a court of law”. It is to that standard and potential outcome that those involved in such examinations have to work. Through the use of highly specialist skills and tools, it is frequently possible to determine what happened where, how and why it happened, and who and what was involved.

Recourse to litigation is generally a last resort for most organisations, so why should you be concerned about potential evidence and related disputes? Forensic evidence could help manage the impact of some important business risks. Forensic evidence can also support a legal defence. For example, it could show that due care was taken in a particular process; it could verify the terms of a commercial transaction; or it could lend support to internal disciplinary actions.

Those who specialise in this field integrate skills in accounting,



information technology, auditing and investigation. Their work ranges from helping investigate actual or alleged fraud to assessing the financial impact of an information security incident (which may in turn be the result of a fire, flood or other disaster). The approach can be seen in three broad areas: forensic accounting, forensic recovery, and digital forensics.

Forensic accounting

Using an in-depth understanding of data and financial reporting systems, accounting and auditing standards and procedures, evidence gathering and litigation processes, and – most importantly of all – tried and trusted investigative techniques and tools, forensic accountants do their work. They are also increasingly playing a more proactive risk reduction role by designing and performing extended procedures as part of the statutory audit, acting as advisors to audit committees, fraud deterrence engagements, and assisting in investment analysis research.

Forensic recovery

Where companies have failed, directors and other parties may have contributed to the collapse through negligence, misconduct, or the misappropriation of assets. In the case of theft of funds it is often feasible to identify the precise amounts involved and trace assets to facilitate recovery. Forensic specialists may thus become involved in recovering proceeds of crime, and in relation to confiscation proceedings concerning actual or assumed proceeds of crime or money laundering. Our team of specialist licensed insolvency practitioners can take a “no win, no fee” approach to investigating and pursuing claims on behalf of creditors, including government agencies. They are experienced in dealing with the requirements of Proceeds of Crime Act restraint and confiscation matters, Civil Recovery investigations and with all aspects of

asset tracing and recovery. They are also experienced in executing search and seizure orders as well as freezing injunctions.

Digital forensics

Almost any activity on a computer, mobile phone or related device leaves evidence of that action, of which most users are unaware. The preservation, identification, extraction, documentation, and interpretation of that evidence are the province of the digital forensics specialist. These experts can assist organisations in such areas as:

- Legal cases, computer forensic techniques are frequently used to analyse computer systems belonging to defendants (in criminal cases) or litigants (in civil cases).
- Recovering data in the event of a hardware or software failure.
- Analysing a computer system after a break-in, for example, to determine how the attacker gained access and what the attacker did.

Previously on this channel...

Consider the case of a finance director who had a new home built. He passed all the invoices through his employer's books, effectively stealing nearly £500,000. Suspicions were aroused whilst he was away on holiday. By examination of the accounts, our team was quickly able to confirm the problem, identify the fraudulent transactions, and – by detailed examination of his computer, including emails and spreadsheets he thought deleted long ago – acquire sufficient evidence to stand up in court. Another recent case involved alleged multi-million pound theft and fraud by former employees of an engineering firm. As would be expected the investigation turned to email correspondence between the alleged perpetrators as well as

documentation held on computer files. The challenge was to search the many millions of emails that had been sent and received by the company over a number of years, as well as a substantial number of files, quickly identify any incriminating evidence, and to ensure that this evidence could be relied on in court.

Of course, it's not necessary to have crime involved to find valuable uses for forensic skills. Our experts have found errors in spreadsheets, recovered data which was accidentally deleted or was on a failed computer's disk drive, and assisted loss adjusters in valuing a company's intangible assets (eg lost business) after a disastrous fire.

Can we help?

Kingston Smith has uniquely had an established multi-skilled forensics capability since 1980. We provide a complete solution, having skills in all the areas outlined in this paper. This eliminates issues such as coordinating the work of separately engaged forensic accountants, IT specialists and recovery experts; and makes the service we provide much more client-friendly and cost-effective.

Our specialist forensic group provide efficient investigatory and dispute consultancy services to individuals, corporate entities, lawyers and professional advisers, regulatory bodies, government and law enforcement agencies and judicial authorities.

The team has been engaged in a wide range of activities including:

- Commercial disputes
- Sale of business disputes
- Shareholder / director or partnership disputes
- Compulsory purchase orders
- Insurance claims
- Professional negligence
- Fraud and financial crime

- Matrimonial disputes
- Personal injury, fatal accident and medical negligence
- Computer misuse

Our highly experienced investigative experts will locate, acquire, analyse and report on forensic evidence.

This evidence may be crucial to your investigation of fraud, intellectual property theft, corporate espionage or unauthorised network access.

Expert Witnesses

These experts have conducted hundreds of investigations and forensic examinations in the UK

and internationally, in both the corporate and law enforcement industries. They have testified as Expert Witnesses in many court cases, and maintain industry leading certifications.

We are regularly recommended by leading barristers and lawyers. The effectiveness of our work has been proven time and time again in cases that have gone to court or have been otherwise resolved.

In order to ensure the integrity of digital data, as a matter of course at Kingston Smith we ensure that the prescribed chain of evidence protocols are maintained throughout the life cycle of an investigation. The preservation of this audit trail is a

key component of the admission of evidence to court or tribunal should it ultimately prove necessary.

We also use the most advanced and effective toolset. For example, in examining spreadsheets, we use the tools developed by HM Customs & Excise to detect fraud and error. When looking at computer disks, we employ the same tools as used by the high-tech crime unit of Interpol.

Experience has shown that the sooner we are involved in an engagement, the better for the client. Please feel free to contact us for advice at no obligation before it's too late!

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP. Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD