

Silent Witness



Almost any activity on a computer 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:

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

The preview process

Any IT forensic examination begins with a preview. Here, the goal is to determine whether or not a given target device has useful (in terms of the investigation) data.

During any computer forensics operation, the state of the target device must be left as undisturbed as possible. This underlying principle applies to all forensic activities, ranging from the field preview to full-blown examination in a lab. Where computer forensics is concerned, the concept of *less is more* carries great weight. The less an investigator has to do to interact with and extract information from evidence (or what may become evidence), the better.

A couple of important guidelines

First, always consider the possible legal ramifications of investigatory activities; consult with your organisation's legal counsel in advance of such activities. For example, some investigations may in certain circumstances constitute a violation of privacy.

Second, document all investigative activities taken. Should the preview process indicate that useful data is present on the target device, the investigator may need to account for the interactions that have taken place as a result of the preview. The

discovery of interesting data does not necessarily translate into a full blown investigation: whether or not a target device suddenly becomes a "crime scene" is contingent on the data itself, organisational policy, and the investigator's judgment. If this happens, the investigator's preview documentation will become the start of a chain of custody.

Systematic examination

Digital forensic investigations typically involve the seizure of a suspect's PC. The hard-drive is imaged in a way which cannot alter



the original; and an investigation proceeds to search for traces of evidence. The examination is conducted in a systematic, formalised and legal manner to ensure the admissibility of the evidence. In legal proceedings, the process of a digital forensic investigation is subject to considerable scrutiny of both the integrity of the evidence and the integrity of the investigation process.

Recourse to litigation is generally a last resort for most organisations, so why should you be concerned about potential evidence and related disputes? Digital evidence could help manage the impact of some important business risks. Digital 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. There are many situations where a simple dispute or information security event may become more serious. If the evidence has not been gathered to begin with, it may be too late to do so later in the process. Therefore, it is necessary from the outset to consider the importance of evidence and to be prepared to gather it for a wide range of scenarios.

Being prepared in this way can also have benefit as a deterrent. A good deal of crime is internal. 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. A company 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.”

Forensic readiness

A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security or criminal incident. In fact, there are many circumstances where an organisation may benefit from an ability to gather and preserve digital evidence before an incident occurs. Forensic readiness is defined as the ability of an organisation to use digital evidence whilst minimising the costs of an investigation. Preparation to use digital evidence may involve enhanced system and staff monitoring; technical, physical and procedural measures to secure data in a way that will stand up in court, processes and procedures to ensure that staff recognise the importance and legal sensitivities of evidence; and appropriate legal advice and interfacing with law enforcement.

Organisations can put in place some simple yet effective measures to help deter computer crime and position themselves to respond to attacks by improving their ability to conduct this type of investigation. These include:

- retaining information;
- planning the response;
- training and awareness;
- preventing anonymous activities; and

- protecting the evidence.

The organisation needs to have planned procedures in place to preserve digital evidence and to instigate a forensic investigation. These in turn should link with the business continuity plan and incident response procedures, as well as the overall security policy and strategy.

Costs and benefits of forensic readiness

If forensic readiness is an enterprise issue, then the extent to which it can be pursued will depend on the organisation obtaining value for money for any investment. The foremost issue in understanding the need for forensic readiness is a risk assessment. An existing risk assessment for something like ISO27001 will be a valid starting point, but may not cover all the situations where digital evidence may be required. An asset register is certainly needed; together with an indication of the attractiveness of targets to the various types of crime such as fraud, malicious damage, and intellectual property theft, as well as an understanding of the impact on the company should such an event take place.

The goals of forensic readiness are as follows:

- to gather admissible evidence legally and without interfering with business processes;
- to gather evidence targeting the potential crimes and disputes that may adversely impact an organisation;

- to allow an investigation to proceed at a cost in proportion to the incident;
- to minimise interruption to the business from any investigation; and
- to ensure that evidence makes a positive impact on the outcome of any legal action.

Any information security defensive measures based on a risk assessment will always leave a residual risk. Often this is because users are trusted not to cause a security incident. In the long run, such an assessment may be correct and stringent defensive measures may not be required. In forensic readiness, however, it is necessary to assume that an incident will occur, even if a risk assessment

Depending on the impact of such an event, an organisation may need to put in place measures to identify any miscreant and obtain the evidence required to take appropriate action against them. Once an organisation recognises that it requires some form of investigative capability, the next step is to ensure the efficiency and competency of that capability.

The costs of implementing forensic readiness may be significant, particularly in an organisation with an immature information security management processes. However, the costs are significantly lowered if the organisation has already performed a comprehensive risk assessment, implemented a business continuity plan, and has factored awareness of information security into staff training.

- updates to policies;
- improvements in training;
- systematic gathering of potential evidence;
- secure storage of potential evidence;
- preparation for incidents;
- enhanced capability for evidence retrieval; and
- legal advice and developing an in-house digital forensic capability, if required.

Dealing with incidents and evidence

In any IT security incident there will be a tendency to focus on containment and recovery, as these are the foremost business critical issues. However, in stressing these, any evidence that might subsequently be required may be damaged, discarded or simply ignored. A lot of information is also lost or discarded as part of normal business practice. Forensic readiness will alleviate this risk to a large extent.

This paper principally focuses on computer fraud investigation, but the principles extend to a wide range of incidents that can impact an organisation: for example, threats and extortion, accidents and negligence; stalking and harassment; commercial disputes; disagreements, deceptions, and malpractice; property rights infringement; economic crime e.g. fraud, money laundering; content abuse; privacy invasion and identity theft and employee disciplinary issues.



says it should not. This is especially true of situations where the risk is highest from insiders. It may not be practicable to deploy preventative measures, especially where staff have to be trusted with high value assets, but effective deterrence may be achieved with forensic readiness.

In a more security-aware organisation, forensic readiness can add value to many existing processes. It may leverage such activities as incident response, business continuity, and crime prevention. The sorts of activities where costs will be incurred include:

There are also potential dependencies and interactions with external organisations to be considered:

- Police (not necessarily the local force, especially if defending allegations from overseas, or if the organisation is multi-national);
- other law enforcement authorities (e.g. HM Revenue & Customs, Trading Standards or Serious Fraud Office);
- overseas prosecution authorities or courts;
- trade union / staff association representatives;
- internal or external auditors;
- regulatory authorities (e.g. Financial Services Authority, Information Commissioner, Bank of England);
- customers, suppliers, partner organisations; and
- the media – due to the need to manage the PR impact of any incident.

At the end of an incident there is a clear need for the organisation to

learn from it. From a forensic readiness perspective there is an opportunity to assess the adequacy of the investigation and the utility of the evidence gathered to support it. Lessons learned need to be relayed to the appropriate people and can help the organisation refine its prevention measures. Learning can also be achieved by tracking evidence recovery within incident handling and response, in the same way an organisation might track business continuity.

Possibly the most significant barrier to forensic readiness is that organisations rarely communicate their risks well enough to allow those who are monitoring the IT systems to collect the most appropriate data. The other main issue is that for a variety of unforeseeable reasons, evidence may be inadmissible or weakened by opposition lawyers.

The field of digital evidence is still new and courts are wary of accepting it. Best practice is still emerging and case law is thin on the ground.

Can we help?

Kingston Smith Consulting has an established computer forensics capability. We use experienced digital investigative experts that will locate, acquire, analyse and report on electronic data. The digital information may be crucial to your investigation of fraud, intellectual property theft, corporate espionage or unauthorised network access.

In order to ensure the integrity of the digital data, as a matter of course we ensure that 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.

These experts have conducted hundreds of digital investigations and computer forensic examinations in both the corporate and law enforcement industries and have testified in many court cases. They maintain industry leading certifications such as Certified Forensic Computer Examiner (CFCE), Certified Information Systems Security Professional (CISSP) and Encase Certified Examiner (EnCE).

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