Information Assurance Advisory Council

IAAC

# Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence

*Second Edition*

*Version 2.1 Jan 2009*

www.iaac.org.uk

**The Information Assurance Advisory Council (IAAC) is a private sector led, cross-industry forum dedicated to promoting a safe and secure Information Society. IAAC brings together corporate leaders, public policy makers, law enforcement and the research community to address the security challenges of the Information Age.**

**IAAC is engaged with Government and corporate leaders at the highest levels; it produces innovative policy advice based on professional analysis and global best practice.**

## Corporate Sponsors

Anite public sector

AIRWAVE

symantec.

Microsoft

UNISYS imagine it. done.

RSA SECURITY

BT

NORTEL

## Government Liaison Panel

CESG

CPNI Centre for the Protection of National Infrastructure

BERR Department for Business Enterprise & Regulatory Reform

csia Central Sponsor for Information Assurance

SOCA

***Disclaimer***

***IAAC's recommendations do not necessarily represent the views of all of its members or sponsors, whether private sector or Government. Strategic interaction with Government is through a Government Liaison Panel.***

# Foreword

As Chairman of the Information Assurance Advisory Council (IAAC), I am delighted to be associated with this updated Guide to Digital Investigations and Evidence for Directors and Corporate Advisors, written by Professor Peter Sommer. The purpose of this guide is to make directors and, managers and their professional advisors aware of the issues involved in collecting, analysing and presenting digital evidence.

The nature of information usage and handling is changing, but our approach to managing it is not. Government Departments are still assimilating the full implications of the wide range of major issues raised in the reports that followed the recent, serious, data losses. These contained many common themes that are equally applicable to the private sector. Each loss has undermined the confidence of individuals in the ability and commitment of Government Departments, agencies and their private sector service providers, to protect their personal data.

The most widely publicised, recent, data losses have involved government departments and their private sector partners. Less well publicised, but significant, data losses continue to occur in the private sector. These failures threaten reputation, trust, business and operational effectiveness, and personal and corporate security. They constitute significant business risks and are, therefore, of direct interest to executive board members and the respective audit committees. Data losses may arise from incompetence or from criminal activity. In either case, failures in process, culture, behaviour, management oversight and overall governance are likely to be contributory factors. This may well be because executives at board level have not fully understood and managed two of their principal business assets – their people and their data – and the risks related to them.

This useful guide highlights the potential risks for enterprises that do not have a detailed planned response to typical risk scenarios. It points out that the 'Low Frequency/High Impact' events are disruptive and emphasises that 'High Frequency/Low Impact' events are also disruptive and must be addressed by contingency plans and preventative measures.

In commending Professor Peter Sommer's clear and informative guide to its readers, I seek to highlight the crucial importance of timely and sound decision making by senior management, taking due notice of the advice given by their technical experts.

Sir Edmund Burton
Chairman, Information Assurance Advisory Council

## About the Author

Peter Sommer (**peter@pmsommer.com**) is a Visiting Professor in the Department of Management, London School of Economics where his specialty is the legal reliability of evidence from computers and he teaches the Information Security course. He is also a Visiting Senior Research Fellow, Faculty of Mathematics, Computing and Technology, Open University where he is course consultant on their Forensic Computing and Investigations course.

His first degree was in law; in the course of a long professional career he has carried out many post-incident investigations, acted as risk analyst for leading insurers and loss adjusters and acted as an expert witness in many leading criminal and civil trials involving complex digital evidence.

Casework has included charges of high-value fraud, industrial espionage, defamation, theft of intellectual property, software counterfeiting and piracy, global computer misuse, large-scale distribution of paedophile material, multiple murder, narcotics trafficking, terrorism, “phishing”, theft of trade secrets, defamation and corruption.

He is a former Parliamentary Specialist Advisor and sits on a number of Whitehall Advisory Panels. He is the joint lead assessor for “digital evidence” under the scheme run by the Council for the Registration of Forensic Practitioners (CRFP) (**www.crfp.org.uk**).

## Disclaimer

This publication is intended to provide a general overview of the issues and to indicate sources of further information. The advice tendered should only be used together with analyses specific to individual organizations and as part of a broader management strategy. Neither Peter Sommer nor the Information Assurance Advisory Council will accept responsibility for any losses or damages incurred as a result of use of material contained in this paper.

## Acknowledgements

A number of people offered comments on the previous edition as well as reading in draft this edition. I wish to thank all of them and particularly Harry Parsonage. I would like to thank IAAC for hosting, and Unisys for supporting, this publication. Any mistakes are my own.

# Contents

## Executive Summary

Nearly all organisations underestimate how often they may be called on to produce reliable evidence of what has happened in and around their information and communication technology (ICT) systems. This may include crimes but more often, civil disputes. Businesses and other organisations also underestimate the demands that the legal system makes in terms of ensuring the admissibility and reliability of digital evidence. Both of these can have a profound impact on business welfare.

The purpose of this Guide is to make directors, managers and their professional advisors aware of the issues involved in collecting, analysing and presenting digital evidence. The first third deals with the main management problems and the remainder provides detail of some of the practicalities of implementation.

**The overall message is the importance of having a corporate Forensic Readiness Program.**

Since the early 1990s and in particular in the wake of the IRA-inspired bombing campaigns, prudent organisations have felt the need to have a Disaster Recovery or Business Contingency Plan. The events anticipated are usually characterised as high impact/low frequency; they don't happen very often but when they do they threaten the continued existence of the organisation.

The purpose of such plans is to reduce the panic, to know in advance who should be doing what to speed recovery, to set up procedures, to buy in external resources and facilities. Even though it is impossible to predict the form and direction of any specific catastrophe, the existence of generic plans is now regarded as essential to survival.

But much more common than the catastrophic event is the one where there is a threatened legal outcome. Examples include disputed transactions, suspected fraud, employee problems, complaints of negligence, "smaller" cyber attacks, theft of data. These may be comparatively low impact but they are also high frequency events; most organisations will experience some form of them over the period of just a few months and some may expect them daily.

Common to all of them is the need for evidence, usually in digital form, to support the organisation's position. Hence the need for a Forensic Readiness Plan, a sibling of the Disaster Recovery Plan.

**If your organisation was asked to provide reliable evidence of what has happened within its computers, perhaps after a suspected crime or attack, or to resolve a legal dispute – how well would it respond?**

There is an unfortunate tendency to label "hi-tech" crime as somehow distinct from other forms of criminal activity. In practice, given the extent to which nearly all businesses and very large numbers of people use computers and other digital devices, there is now an extraordinary range of circumstances in which a criminal investigation may need to follow up evidence in some digital form. And that can include such unobvious categories as murder, narcotics trafficking and terrorism. Increasingly therefore, the problem is not “How do we tackle hi-tech crime?” (which then invites the problem of defining the precise scope of “hi-tech crime”) but how do we embed into our regular investigative processes the specific skills and resources needed to handle evidence in digital form?

A few figures from National Statistics tell us the extent to which businesses and individuals depend on ICT: in 2005, 93 per cent of businesses in the UK with ten or more employees reported using personal computers or similar devices; in 2006 70 per cent of UK businesses had a website, just over 50% interacted with central and local government over the Internet, just under 15% *sold* over the Internet and 57% made purchases. 57% of all UK households had internet connectivity and 70% of those did so over broadband. By June 2008, broadband connections were up to 93% of the total. In the middle of 2008 a well-specified personal computer could be bought for the equivalent of 3 days’ earnings of some-one earning £30,000 pa. Costs of personal digital storage, a key indicator of how much data is easily retained (or covertly stolen) had dropped to 10p/GB for external hard-disks. 1 GB of hard-disk could be 100,000 items of correspondence or 20,000 medium resolution pictures. The document you are reading occupies 0.002 GB on a hard-disk.

The detail of the problems that arise when an organisation needs to produce evidence may be “techie”, but the implications for the continued smooth running of the organisation require proper control from, and the full understanding of, the organisation’s most senior decision-makers.

Evidence is required in a very wide range of circumstances, for example:

- in disputed transactions;
- in allegations of employee misbehaviour;
- to show compliance with legal and regulatory rules;
- to avoid charges of negligence or breach of contract;
- to assist law enforcement in criminal and anti-terrorist investigations;
- to meet disclosure requirements in civil claims;
- to support insurance claims after a loss.

“Forensic Computing” is now an established set of disciplines and the very high standards now in place for preserving material from personal computers create high expectations of other forms of digital evidence, including those from large corporate systems and networks, across the Internet and the families of personal digital assistants (PDAs), mobile phones and portable media units.

Unless the organisation has developed a detailed planned response to typical risk scenarios, much potential evidence will never be collected or will become worthless as a result of contamination. Moreover, during an investigation, the organisation will be constantly faced with a dilemma: lose business when essential systems are switched off so that evidence can be properly preserved; or be profoundly handicapped and incur losses because evidence cannot be produced.
What is needed is a forensic readiness plan.

The first part of this guide is directed at major decision-makers, corporate strategists and their senior advisers, including lawyers. It covers the following:

- **explaining the legal requirements of "evidence" and the problems of admissibility;**
- **showing the life-cycle of incidents and how evidence collection needs to be integrated into regular crisis management, incident response and litigation plans;**
- **showing the management planning, processes and disciplines necessary if an organisation is to emerge with the greatest possible range of options;**
- **providing a scheme for deciding the resources that will be required and when and how far requirements can be outsourced to specialist third parties.**
- **the handling of obscene and paedophiliac material;**
- **the handling of encrypted material**
- **points of contact in law enforcement agencies;**
- **pointers to further information;**
- **a glossary**

In effect there is a seven-step process:

- **identify the main likely threats faced by your organisation**
- **identify what sorts of evidence you are likely to need if you have to proceed to civil litigation or criminal proceedings**
- **identify how far you may have that evidence already**
- **identify what you will need to do to secure additional essential evidence**
- **familiarise yourself with potential legal problems such as admissibility, data protection, human rights, limits to surveillance, obligations to staff and others, disclosure in legal proceedings**
- **identify the management, skills and resources implications for your organisation**
- **turn the results into an action plan – which will need regular revision as the organisation and its ICT infrastructure develops.**

Throughout this guide background and more technical detail is omitted from the main narrative but appears in the second half as a series of appendices. The guide cannot give more than an overview of the issues as they apply to a wide range of generic organisations. Success will depend on the extent to which directors and senior managers take these ideas forward and adapt them to the specific needs and features of their own organisations.

Lawyers called upon to provide detailed guidance will also find some of the technical material on types of evidence and methodologies for acquisition helpful.

Although this guide is designed for use within the United Kingdom and the descriptions of the law refer to English law, many of the principles are universal in all jurisdictions.

----------------------------oooo-----------------------

In the three years since this guide first appeared there has been a radical alteration in the way in which UK law enforcement agencies respond to "hi-tech" crime. There is no longer a National High Tech Crime Unit (NHTCU) but the Serious and Organised Crime Agency (SOCA) has an E-Crime Unit and arrangements within the various police forces are having to be changed as well. From Spring 2009 onwards there should be a Police Central e-crime unit (PCeU). One of the minor consequences is that the old NHTCU website, a source of useful advice and documents and upon which the first edition of this guide had rather relied, ceased to exist in April 2006. For those organisations which are part of the Critical National Infrastructure, NISCC has been absorbed in the Centre for the Protection of the National Infrastructure, CPNI. Information and Communications Technology (ICT) has continued its rapid evolution and this is having an impact on how investigations involving digital evidence are carried out. Increasingly closed circuit television (cctv), a vital resource of physical security and which used to be archived to video tape, is now digitally stored and hence capable of digital examination. Telephony based on internet protocols (VOIP) is no longer a mere geeky experiment but a substantial and growing alternative for businesses and private individuals – there are many problems of how evidence from VOIP may be collected and handled. More and more companies are routinely recording telephone traffic, but there are both technical and legal problems associated with its use in court. Mobile telephones and PDAs are converging in functionality so that the day of "ubiquitous computing" – any information anywhere – is upon us. There have been some important amendments to relevant law. We now have in place measures which require businesses, in particular circumstances, to assist law enforcement agencies in the handling of encrypted material. There are also extensions to the law involving pornographic material.

All of these reasons have persuaded us to issue a substantial new version of the guide at this point rather than simply carry on updating the downloadable file that has been available on the IAAC website. We have also taken the opportunity to add some new features, including appendices on the powers of civilian investigators, cctv and handling encrypted material.

# 1 Introduction: the Need for Digital Evidence

As more and more transactions from the commercial world, government and private individuals exist only in digital form, the only way in which you can prove that something has happened – or failed to happen – is via digital evidence. In the digital world people leave digital footprints of their activities from which their actions and intentions can be inferred.

But digital evidence is often highly volatile and easily compromised by poor handling. The chances of success in litigation or successful criminal prosecution by law enforcement agencies depend heavily on the availability of strong evidence. Failure in civil litigation means financial loss, including legal expenses; a failed criminal prosecution can also generate reputational damage to a victim. While many sensible organisations have arrangements in the event of fire, flood, failure of electricity and telecommunications services or acts of terrorism, very few have thought-through plans to identify, collect and preserve digital evidence in forms which will prove robust against testing in legal proceedings.

Yet demands for digital evidence are far more common than any of the subjects of conventional disaster contingency planning. Very few organisations have the management structures in place to enable them to carry out an efficient, cost-effective and low-impact digital investigation.

Following some of the major financial scandals of the late 1990s and early 2000s, new strands of legislation and regulation impose on businesses the requirement to produce and preserve a wide variety of business records. In the best known of these, the US Sarbanes-Oxley Act of 2002, there are explicit penalties for deliberate destruction of certain essential files. The Basel Committee on Banking Supervision Revised International Capital Framework of 2004 ("Basel II") requires companies in the financial services industry to conduct a broad risk assessment of those to whom it makes loans or in which investments are made[1]. The UK Combined Code of Corporate Governance applies to quoted companies and lists a wide range of compliance requirements, including operation issues and risk management[2]. An undercurrent to these and similar items of legislation and regulation is that material produced in electronic form is reliable. Forensic compliance services are already being set up to maintain reliable archives of essential business documents and emails, but their remit is limited. In the UK, the Freedom of Information Act 2000 states that all public sector bodies must supply requested information within 20 working days, and that such information has to be "reliable".

During 2007 and 2008 a number of UK government departments suffered catastrophic compromises of security: losses of computers, memory sticks, CDs. A series of reports followed: Poynter on the loss of 25 million HMRC records on two CDs[3], Burton on events at the Ministry of Defence[4]; Thomas/Walport on Data Sharing[5] and

[1] Http://brief.weburb.dk/frame.php?loc=archive/00000141/

[2] Http://brief.weburb.dk/frame.php?loc=archive/00000147/

[3] http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf

[4] http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/ReportIntoTheLossOfModPersonalData.htm

Hannigan on Data Handling Procedures in Government[6]. Common to all of these was an emphasis on the need for formal Information Assurance policies, changes in corporate culture and the need for stronger scrutiny of security performance. Implicit rather than explicit in all of these recommendations is the need to be able to prove that appropriate levels of care have in fact been exercised.

This guide aims to help directors, senior managers and their legal advisers to understand the key strategic and management issues. It is designed to anticipate the need for provision of digital evidence and investigations by setting up management procedures, acquiring appropriate resources and identifying third-party sources of emergency assistance. For lawyers, it provides an overview of the types of digital evidence and the associated problems of probative value, admissibility and disclosure. But it is only a starting point – other, more specialist publications will need to be consulted while a detailed plan is formulated.

While the detail of collecting and analysing digital evidence is substantially a matter of deploying technical skills, success in doing so depends heavily on the level of careful pre-planning. As we will see, in the middle of an incident there are often important choices to be made between the proper preservation of evidence – which may involve shutting down central computer services for the duration – and the continuity of the business. These are decisions for the business's most senior managers, not computer technicians or hurriedly-hired external consultants. Again, if planning is poor, key personnel may find themselves being diverted into supporting investigatory and legal processes instead of running the business. The text and appendices to this guide will help to start the process of establishing a proper corporate strategy.

[5] http://www.justice.gov.uk/docs/data-sharing-review.pdf

[6] http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx

# 2 Digital Investigations and Digital Evidence

The triggers for digital investigations are not confined to the obvious cybercrime spectaculars which capture media attention. Far more common are relatively low-level events such as contractual and employment disputes which, if not handled properly, can still cause considerable direct and indirect losses to organisations. One or more of these events will happen to most organisations within any given year, and the triggers for these can include suspected, attempted or actual:

- **frauds perpetrated by employees or third parties;**
- **contractual disputes;**
- **allegations of breach of duty of care;**
- **email and Internet abuse;**
- **online defamation;**
- **employee disputes;**
- **sexual harassment;**
- **acquisition and storage of pornographic and paedophiliac material;**
- **theft of confidential data, data theft and industrial espionage;**
- **theft of source code and software piracy;**
- **unauthorised access by employees;**
- **unauthorised access by outsiders ("hacking") and unauthorised data modification (viruses, Trojan horses, etc.);**
- **theft of corporate computer resources for private exploitation;**
- **use of corporate computer resources to facilitate file-sharing which violates third-party intellectual property rights or are obscene or indecent;**
- **use of corporate computer resources as one stage in a complex criminal act and where a third party is the intended victim;**
- **failure of an organisation's computer systems, causing damage to third parties and giving rise to legal claims for breach of contract or in negligence;**
- **failure of an organisation's computer systems such that the organisation wishes to sue suppliers for breach of contract;**
- **extortion attempts, whether based on physical threats or logical attacks such as distributed denial of service;**
- **"phishing", where someone is induced to give away important confidential information to a fake website – businesses may either lose information in this way or find that their own website is being mimicked by phishers;**
- **denial of service and terrorist-motivated attacks; and**
- **insurance claims arising out of the above.**

Traditional disaster contingency plans prepare for Low Frequency/High Impact events. These can occur in the ICT domain as well, but one has also to prepare for High Frequency/comparatively Low Impact events.

Organisations can find themselves pulled into computer investigations against their will. In civil proceedings the other party is often entitled to demand disclosure or discovery of computer-derived materials. In criminal proceedings, even though the organisation may be a victim or otherwise a wholly innocent bystander, requests for disclosure from a computer system may be made by the defendant's legal team.

Attempts at investigation involving computers often fail because of mistakes made at a very early stage – essential digital evidence is ignored, destroyed or compromised and suspects are inappropriately handled. The very fact of having to start such an investigation can create a crisis within a victim organisation. The crisis then needs to be managed. These are some of the main questions that will need to be addressed and which we will be considering later:

- **To whom should initial suspicions be reported?**
- **Who runs the investigation within the organisation?**
- **Who needs to be involved?**
- **How should the investigation be carried out?**
- **What important procedures need to be followed?**
- **What are the characteristics of good evidence?**
- **What steps are necessary to identify "relevant" digital evidence – and once located, how can it be reliably preserved?**
- **What legal obligations exist during such an exercise?**
- **What may third parties be able to demand by way of "disclosure"?**
- **How can the investigation operate effectively without hindering day-to-day activities or promoting a crisis of confidence with greater potential for damage than the original wrong?**
- **How much external help is needed – and what kind?**
- **Do suspected crimes always need to be reported to the authorities?**
- **Once a suspicious incident has been reported, how should the relationship with law enforcement and the courts be managed?**
- **How does an organisation's senior management retain control of the agenda and direction of an investigation? And how does it relate this to its top-level obligations to keep the organisation's business functioning normally?**

The arrangement of this guide is as follows. First, it looks at the life-cycle of incidents and investigations: without an appreciation of organisational activity, planning is impossible. Second, it develops an understanding of the various overall management aims during an incident so that possible conflicts can be identified (and hopefully be resolved in advance).

Third, the likely risk scenarios that might face a specific organisation are identified. This process has something in common with traditional security and contingency planning analysis. The aim here is not to develop preventative or detective measures, but to elucidate the kinds of digital evidence that are likely to be required for each scenario.

Finally, the general characteristics of “good” evidence and the particular problems of handling digital evidence are considered, and the main types identified.  These aspects inform us as to the standards that need to be strived for, and the traps that may snare an organisation if it fails to consider the types of evidence likely to be required.

With this groundwork, directors and senior managers should be in a position to devise a corporate plan of action that is specific to their organisation.  This has to cover risk analysis, management aims, management structures (including appropriate reporting), core procedures and resourcing.

# 3 Life-cycle of incidents and investigations

No two computer investigations are identical. However, the timeline (see Figure 3.1) gives an indication of the number, complexity and duration of typical corporate tasks that may occur, and for which a management framework is essential. The actual details may vary considerably. It is only possible to grasp the range and extent of management decisions that may be involved during and after a computer investigation by understanding the elements in the life-cycle.

The following section concentrates on what happens in an "incident", but a number of the features in the timeline will also apply in other circumstances, for example, if there is an unexpected third-party demand that digital evidence of various types be produced. In practice, many of the tasks enumerated here will operate concurrently; for some there will be successive bursts of activity and inactivity (Table 3.1).

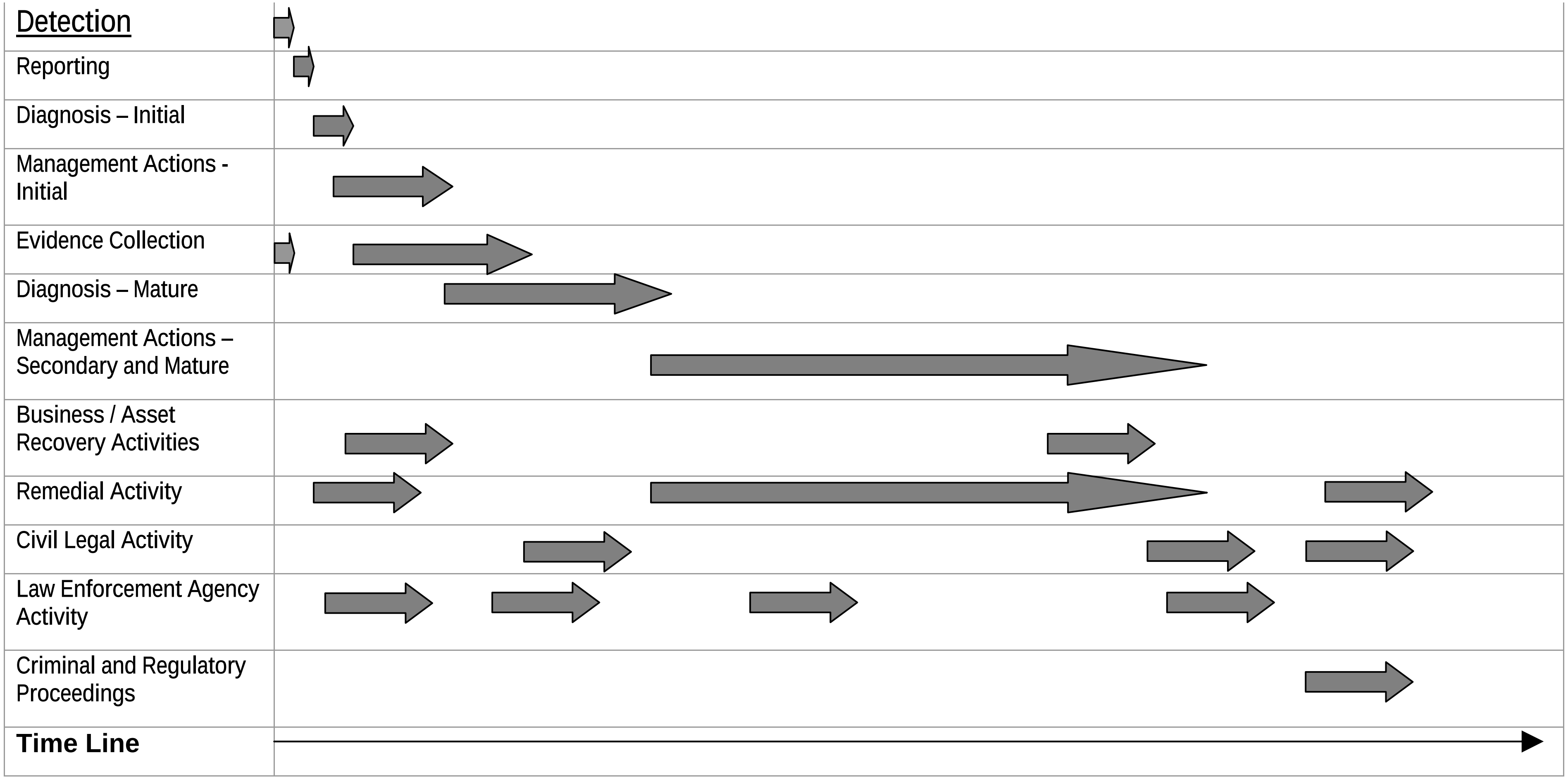
**Table 3.1: Incident Lifecycle**

| | |
|---|---|
| **Detection** | Detection may be prompted by a dramatic event, such as the arrival of an extortion demand, obvious failure of major services. Or it could be no more than a suspicion triggered by anomalous behaviour. |
| **Reporting** | All organisations need a designated point to which reports can be made, whether corporate security, computer security, audit, the company secretary, human resources or a legal adviser.<br>Although reporting is shown here as a single event, in practice the full extent of an incident may take some time to evolve, so there could be several reports. In addition, some reports will turn out to be false. |
| **Diagnosis – initial** | Whoever receives the report should have the skill, experience, resources and corporate clout to make an assessment of what may have happened and to provide initial guidance about how the organisation should tackle the problem. |
| **Management actions based on initial diagnosis** | At this point, the relevant executives will be informed and staff detailed to carry out specific tasks. This will usually involve setting up a special "taskforce". |
| **Evidence collection** | This is one of the most important early stages. It includes identifying likely sources of evidence, collection under controlled conditions and preservation. |
| **Diagnosis – mature** | Initial diagnoses are likely to be wrong. Evidence collection soon moves into evidence assessment, with a consequential effect on how the problems are perceived.<br>Few crises are so purely computer-based that the only kind of evidence is obtained from computers. The ongoing process of diagnosis will take in evidence from and about individuals and businesses and paper-based documents. |
| **Management actions based on mature diagnosis** | As the nature of the problem becomes clearer, the organisation is able to define its objectives with greater clarity and certainty. Once the immediate risks to the integrity of information systems have been resolved, corporate aims will have a more long-term focus. In the timeline, "mature management action" does not cease until the very end, once lessons have been learned. |

| | |
|---|---|
| **Business/asset recovery activity** | If computer systems have been compromised, there has been some interruption to business, assets have been lost or some aspect of the crisis has become public, there will need to be a business recovery phase, similar to that after premises have been affected by fire or flood, or after a conventional theft.<br>Experience from the established disaster recovery/business contingency planning industry suggests that full recovery always takes much longer than expected.  Typical tasks include: restarting computer systems; recovering lost assets; and public relations. |
| **Remedial activity** | This includes learning lessons, preventing repetition, introducing new management and audit procedures, and new security engineering facilities.<br>But you can't learn lessons unless you have fully investigated what went wrong;  these lessons may extend beyond the immediate events to problems with corporate culture and management structure |
| **Civil legal activity** | This covers, for example, insurance claims, asset recovery, claims for damages, negligence, breach of confidence, etc. |
| **Law enforcement agency activity** | There may be several phases of law enforcement activity: initial enquiries; collection of statements and evidence; return visits for further interviews and search for evidence; preparation for trial; and attention to defence requests for disclosure. |
| **Criminal and regulatory proceedings** | A complex criminal trial may go through several phases, including committal and the substantive trial.  Further information may be requested during the trial process. |

As can be seen, the value of evidence in the overall recovery plan is towards the end of the process, after all the more immediate actions have been taken.  But to be truly effective, evidence identification and collection needs to commence at a very stage within an event.

## *Life-Cycle of Incidents*



**Detection**

Reporting

Diagnosis – Initial

Management Actions - Initial

Evidence Collection

Diagnosis – Mature

Management Actions – Secondary and Mature

Business / Asset Recovery Activities

Remedial Activity

Civil Legal Activity

Law Enforcement Agency Activity

Criminal and Regulatory Proceedings

**Time Line**

# 4 Overall Management Aims

The types of event with which we are dealing here fall outside the mainstream activities of most organisations. The normal delicate balance of conflicting requirements within an organisation is placed at hazard whenever there is an unexpected crisis. What we are concerned with is not revenue or profit generation, but loss mitigation. A computer-related investigation is usually triggered by a crisis but can become one in its own right. Once an organisation decides to anticipate the problem there are issues about the adequacy of setting the right levels of resource. Against the risks of being unprepared are the risks of expenditure on facilities and personnel that may never be used.

Up to a point all crises, however set-off, have common features and can be handled through a common business continuity plan. So it may not matter whether a business interruption is caused by a fire, flood, terrorist action or telecommunications service failure – individual detailed business continuity plans for each of these scenarios would be very similar.

The first duty of an organisation is to survive so that it can continue to serve its customers and clients, meet its obligations to debtors, bankers, employees, the public at large and the state. In addition, commercial organisations are expected to generate profits for shareholders. Typical top-level aims during a crisis include:

- arranging for the organisation to continue with its main activities;
- rapid recovery to full operational status;
- recovery of any organisational assets that are at hazard;
- successful insurance claims;
- successful legal claims against third parties;
- meeting obligations to third parties;
- assisting law enforcement in potential criminal matters;
- realising the largest possible number of options for the organisation in terms of future action.

Not least of the difficulties is that, in computer investigations, management objectives may change as more is learned about what has taken place. In particular there will be significant conflict between the need for organisational continuity and the requirement to collect evidence reliably from the very machines that keep the organisation operating.

So, an organisation needs a management and executive framework within which crisis decisions can be made. Some key questions for consideration are as follows.

- To whom should initial reports be made?
- How is an emergent problem to be diagnosed?
- Who will assess the overall impact on the organisation?
- How will the organisation’s main management be in a position to arbitrate the key decisions?
- Who will pursue in detail the investigation, the recovery, the liaison with third parties, the possible public relations impact, the legal aspects?

Many larger organisations already have contingency plans for fire or flood, bombing, kidnap or malicious tampering with a product, for example. But there are also a number of unique features, examined below, which will need to be addressed separately. Before describing the complexion of a planning team and its role within an overall management structure, the nature of the task that it faces needs to be appreciated.

Further, the organisation will need an executive resource. This may be an existing security or contingency planning unit or extensions thereof, perhaps even a completely new unit. Each organisation will need to make its own decisions according to its needs. Finally, there is the question of how extensive that resource should be: does it require its own in-house forensic computing expertise, or can it rely on third parties, or should there be a combination of the two?

# 5 Risk Scenarios

The types of evidence that an organisation may need to collect and the methods that it uses to carry out the acquisition emerge from carrying out risk scenarios.

All prudent organisations develop their security policies on the basis of risk analysis. They collect data on the threats that their type of business might face and try to rate each hazard in terms of the frequency and cost of each potential incident. In regular security analysis, the outcome is usually a set of preventative and detective measures. In some instances, measures to mitigate damage and recover losses are added to these. The types of measures selected will include administrative changes, audit controls, the deployment of appropriate technologies, contracts for disaster recovery sites and insurance.[7] Usually it is not possible to produce risk analysis against precise financial metrics because of the lack of accurate actuarial data – and beyond a certain point, too much effort in risk analysis is counterproductive. However, informed approximations are extremely helpful. For example, the estimated annual costs of likely breaches of security can give a strong pointer to a prudent annual budget for security measures. Risk analysis is the essential precursor to sound, panic-free risk management.

But, as it is usually practised, regular risk analysis often fails to identify the types of evidence that could and should be captured. In addition, various lower level situations – for example, disputes about transactions or employment – fall below the horizon of conventional security analysis. So, it is desirable to review all the threat scenarios from the evidence perspective and consider how it will be collected and preserved to a sufficient degree. A scenario consists of starting with a likely triggering event and then playing out, as a paper exercise, all the likely consequences and possible reactions.

For example, consider a scenario for computer disaster recovery. An essential computer service goes down (due to one of various reasons: failure of hardware or software; a fire in the building; a distributed denial of service attack). Playing out the scenario tells an organisation how soon the business becomes unable to respond to queries, the point at which revenue streams become affected, how quickly existing emergency procedures will begin to offer prospects of return to normal working, and what losses will have been incurred in the meantime.

Existing risk scenarios as well as others need to be examined from the evidence perspective. This means being able to relate activities of potential interest to the computer resources on which the activities are being carried out, and developing an understanding of the files that are being created. For each plausible risk scenario an organisation should create documentation identifying the computer resources and associated files which are likely to be of interest. For example, most businesses are vulnerable to fraud, both from employees and third parties. To prove what has happened an organisation will need at the very least the main transaction records, even if the *modus operandi* is not explicitly via a computer. If the activity is computer-mediated, access control logs, web logs and intrusion detection logs will be

[7] See for, example, *Risk Management and Accreditation of Information Systems*, published by the Centre for the Protection of the National Infrastructure (CPNI) http://www.cpni.gov.uk/Products/bestpractice/3016.aspx

needed. In an employee dispute, emails, activity logs, telephone logs and access control logs may be necessary. But each business is unique and there is no substitute for doing the analysis for each plausible scenario.

It is beyond the scope of this guide to provide an exhaustive list of all the potential sources of evidence and their importance in every conceivable type of business operation. However, it is possible to identify certain baseline capabilities which the organisation needs to be able to develop. Many of these are existing records and logs, but the organisation needs to know precisely how to turn them into evidence which is unimpeachable in terms of reliability (see Table 5.1).

**Table 5.1: Potential sources of evidence**

| | |
|---|---|
| **Main transaction records** | These include all purchases, sales and other contractual arrangements at the heart of the business. |
| **Main business records** | These include all of the above, but also all documents and data that are likely to be necessary to comply with legal and regulatory requirements. |
| **Email traffic** | Emails potentially provide important evidence of formal and informal contacts. |
| **Selected individual personal computers (PCs)** | If individuals are under any form of suspicion, the organisation will need to be able to seize their PCs and make a proper forensic "image", which produces a precise snapshot of everything on the hard disks (this includes deleted material which technicians may be able to recover). |
| **Selected cellphones / PDAs etc** | These devices can hold substantial amounts of data. Technical methods for preserving and investigating them are more complex than those for PCs; in addition there may be additional legal problems as ownership and privacy rights may not be wholly clear |
| **Selected data media** | Most computer users archive all or part of their activities on external storage media. These include CDRoms, Digital Versatile Discs (DVDs), floppy disks, tape, external hard disks and Universal Serial Bus (USB) thumbdrives. There needs to be a routine for identifying all of these and securing them, pending examination. |
| **Access control logs** | All but the simplest of computer systems require a password or authenticating device before allowing admission. Usually, these access control systems can be configured to maintain records of when usernames and passwords were issued, when passwords were changed, when access rights were changed and/or terminated. In addition, many systems also maintain logs of accesses or, at the least, of failed accesses. These logs, properly managed and preserved, are powerful evidence of tracking activity on a computer system. |
| **Configuration, event, error and other internal files and logs** | All computers contain files which help to define how the operating system and various individual programs are supposed to work. In the current generation of Windows systems, the most important set of configuration information is the registry. From this, forensic technicians can discover a great deal about recent and past activity, including recently accessed files and passwords. Often, there are important configuration files associated with individual programs. Many operating systems also generate error and other internal logs. |

| | |
|---|---|
| **Internet activity logs** | Individual PCs maintain records of recent web access in the form of the history file and the cache held in the temporary internet files folder. But many corporate networks also maintain centralised logs, if only to test quality of service and check against abuse. When properly managed and preserved, these logs are powerful evidence of activity on a computer system. |
| **Anti-virus logs** | Related to these are logs created by corporate installations of anti-virus software. These record the detecting and destruction of viruses and "trojans". A common defence tactic is to suggest that suspicious behaviour has been caused by a rogue program; anti-virus logs often contribute to resolving such claims. |
| **Intrusion detection logs** | Larger computer systems often use intrusion detection systems as part of their security measures – they are intended to detect and prevent several forms of hacking. Producing such logs may help to identify perpetrators, or demonstrate that reasonable precautions have been taken to secure the system. |
| **Back-up media** | All computer systems need to have back-up procedures, if only to enable rapid recovery after a disaster. Some organisations back up their entire systems every 24 hours; others have in place a partial, incremental policy.<br>Back-up archives are extremely important sources of evidence, as they can show if "live" files have been tampered with. They can also provide data which has been deleted from the "live" system. |
| **Telephone logs** | Private Branch Exchanges (PABXs) usually have extensive features for recording usage activity. There may be difficulty in using these in evidence; there are also significant problems associated with intercepting the content of conversations. However, but these are potentially very important sources of intelligence and evidence. |
| **Telephone Recordings** | Many companies routinely record conversations between their staff and customers, for such reasons as protection against disputed transactions, staff training and "customer relationship management". As above, there may be significant problems associated with intercepting the content of conversations and using them in evidence |
| **Physical security access control logs** | Many buildings control physical access by the use of swipe cards or other tokens. There may be additional facilities to deal with parking or to give access to particularly sensitive areas. There is usually a central control system which generates logs – this can be extremely useful in pinpointing individuals' movements. |
| **CCTV recordings** | Until recently cctv material was stored on tapes in analogue format. But the cost of digital storage – to fast hard-disk – has plummeted. Digital storage means that cctv images can be rapidly identified by date and time of incident. In addition motion detection and other analytic software can be deployed. At the same time the cost of cameras has collapsed as well, so that many more locations can be made the subject of surveillance |

A useful distinction can be made between material which ought to be routinely collected and available, for example, in the form of regular audit logs and additional capabilities for in depth surveillance. Here, an organisation pre-identifies certain categories of evidence, has facilities and procedures for acquiring and collecting it, but only does so against a specific need. There are two main reasons for doing this: (1) there is little point in collecting vast quantities of data against a very limited need; and (2) it is very likely that the more intrusive forms of data collection will need to be justified in law against a proportionality test. So, depending on the circumstances, increased surveillance of, for example, web usage would need to be justified against reasonable suspicion of abuse. (The main legal issues are explored in more detail in Appendix 4.)

It is reasonably well-known that when computer data is deleted it is often readily recovered. This applies to varying degrees to data on the hard disks of personal computers, PDAs, file servers and large corporate machines. Significant expertise in forensic digital data recovery now exists and can be applied both to substantive documents and to the various logs and configuration files mentioned previously. Data recovery is even possible if a disk has been reformatted and partially overwritten with a new "installation". In forensic digital data work, some forms of recovery are trivially easy, whereas others may require high levels of skill and result only in data fragments, the precise significance of which may see some disagreement among experts.

For each item of desirable evidence, an organisation's evaluation and procedures need to reflect answers to the following.

- **How will the evidence be acquired, physically and practically?**
- **How will the evidence be preserved, and how will continuity be demonstrated?**
- **Are there any legal obstacles, such as data protection, human rights legislation or compliance with interception legislation such as the Regulation of Investigatory Powers Act 2000?**
- **Will the material be admissible?**
- **Are there likely to be any problems over disclosure?**
- **Where an organisation has had to rely on forensic digital data recovery, will the results be unambiguous?**

The situations where these questions produce disappointing answers should prompt anticipatory action to be able to "cover" the position with more reliable sources of evidence. (Appendix 2 provides some detail on how various classes of digital evidence may be reliably acquired and preserved. Some of the legal issues are discussed in the next section.)

# 6 “Good” Evidence

Digital evidence must have all the attributes of other types of admissible evidence. Computer-derived evidence provides a number of challenges for the courts and for forensic procedures in general. To understand some of the issues, it is useful to consider what “evidence” is in general terms.

Evidence is that which is offered before a court to persuade it to reach a particular view of events which may be in dispute. In general, evidence may be:

**real** – an object which can be brought to court and examined on the spot;

**testimonial** – the eyewitness observations of someone who was present and whose recollections can be tested before the court;

**documentary** – a business or other record in any form which, once its authenticity has been proved, can be examined for content;

**technical** – where a forensic technician has carried out some procedures on original “real” evidence and has produced some results. Technical evidence, in the eyes of the court, is not the same as expert evidence, which also includes giving opinions;

**expert** – the opinions of someone who is expert in a particular field and/or the conclusions of that expert after carrying out a specific investigation;

**derived** – a chart, video, etc. created from primary evidence to illustrate how certain conclusions might be drawn.

Evidence presented in court has to satisfy tests which fall into two main categories, admissibility and weight.

## 6.1 Admissibility

For evidence to be admissible, it must satisfy certain purely legal tests of acceptability. This tends to be a function of jurisdictions derived from the English common law as opposed to those based on European civil codes. The best known of the admissibility rules are:

the **“hearsay”** rule, which excludes reports of reports;

the **“fairness in evidence acquisition rule”,** which grants discretion to judges to exclude material obtained, for example, in violation of the codes of conduct in the Police and Criminal Evidence Act 1984 and Police Act 1997; and

the **broad testimonial rule** that exhibits including documents need to be produced into court by a human witness who can be cross-examined.

The actual rules are quite complex and have many exceptions. In the UK, intercepted data content can be used only for intelligence purposes – it cannot be admitted in evidence for a court to consider[8]. There is however a fair wind behind those who wish to get rid of this very odd rule, at least in cases involving serious crime and terrorism. In the US the Federal Rules of Evidence help to define “admissibility” in that jurisdiction; US court decisions have produced special rules, not replicated

[8] Regulation of Investigatory Powers Act 2000, see also p. 60 below.

elsewhere, to deal with the admissibility of novel scientific and technical evidence[9]. In most European countries, where criminal procedure is dominated by the notion of an examining magistrate, admissibility rules are either absent or informal, depending largely on a “relevancy” test. In English criminal law, judges have a discretion to exclude evidence unfairly acquired.[10]

## 6.2 Weight

Having satisfied the admissibility criteria, the evidence can be considered then for weight of fact – its persuasiveness or probative value. While in the final analysis “weight” is a non-scientific concept, there are a number of desirable features in non-testimonial evidence, that is, exhibits and documents of various kinds. These attributes include that an exhibit is:

**authentic** – specifically linked to the alleged circumstances and persons;

**accurate** – free from any reasonable doubt about the quality of procedures used to collect the material, analyse it (if appropriate and necessary) and introduce it into court. It has to be produced by someone who can explain what has been done. If a forensic method has been used it needs to be “transparent”, that is, freely testable by a third-party expert. In the case of exhibits which themselves contain statements – a letter or other document, for example – “accuracy” must also encompass accuracy of content. This normally requires the document’s originator to make a witness statement and be available for cross-examination;

**complete** – it tells within its own terms a complete story of particular set of circumstances or events.

## 6.3 Continuity of Evidence

Also known as “chain of custody” in the US, continuity of evidence refers to the ability to report everything that has happened to an item of evidence from the point at which it was acquired to when it is presented as an exhibit in court. Thus, for a knife found at a scene of crime, continuity would be established by means of police notes, photographs, “bagging and tagging” of the knife in a polythene bag with the number of the tag recorded, a witness statement from an exhibits officer, and witness statements from each forensic scientist looking for blood, fingerprints, DNA, etc., which include references to handling the “bag and tag” as well as further witness statements from any forensic scientists instructed by the defence team. The process is designed to limit the opportunities for contamination or confusion, accidental or deliberate, or to pinpoint when contamination occurred. But there are also other elements which set computer-derived evidence apart, as follows.

[9] The *Daubert* tests – *Daubert* v. *Merrell Dow* 509 U.S. 579 (1993) provides the following tests: (1) whether the theory or technique can be (and has been) tested; (2) the error rate associated with the method; (3) publication in a peer-reviewed journal; and (4) whether the technique has gained widespread acceptance.

[10] s 78 Police and Criminal Evidence Act, 1984.

### 6.3.1 Computer data can be highly volatile

Many forms of conventional evidence are claimed to be a “snapshot” of a particular set of circumstances, but the problems are particularly acute with computers. This can create considerable difficulties over authentication as to the content and time of creation.

### 6.3.2 Alteration of computer data

Computer data can be easily altered without leaving any obvious trace that such alteration has taken place. Alterations in handwritten and typed documents are usually self-evident; log and account books are designed so that it is easy to detect whether an entry or page has been omitted. It can be argued that there are plenty of examples of forgery based on typed and handwritten originals, but computer-based documents can be forged with an ease and freedom from detection which is of a quite different order. It is of course entirely possible to design a computer system that thwarts certain forms of unacknowledged alteration. But, in contrast to, for example, paper-based accounts books, there are few obvious “standards” which set a measure of what to expect.

### 6.3.3 Contamination of computer material

As a result of the process of collecting it as evidence, computer material can be easily changed. Many forms of forensic examination run the risk of contamination. Biological samples from a subject can be intermingled with those of the examiner. But the problems with some computer-derived material are intense – the very act of starting up a computer or opening an application or file, even if there is no intention to alter anything, will create changes although they may not be immediately visible.

### 6.3.4 Reading computer evidence

Much immediate computer evidence is not obviously readable by humans. Actual exhibits are often derived, manipulated and “presented” away from their point of origin. This becomes apparent as soon as one moves from the limited vision of “computer evidence” as being simply a “record or document produced by a computer”. There is nothing wholly unique about this; the typical DNA trace exhibit is not DNA itself but a purported representation in a form which aids analysis. The particular problem in relation to computer evidence is that a large number of possible and potentially “accurate” representations of original computer data can exist. What is seized may be a computer hard-disk which in turn contains large numbers of directories of files of various kinds, while what is put immediately before the court may be any of a number of purportedly accurate printouts or “screen dumps”. The large variety of possible representations of original material makes difficult the evolution of “standards” such as those existing for DNA charts, for example. And the possibilities for inaccurate representation are very much greater. Nearly always, computer-derived exhibits require that the court makes a chain of inference before reaching a conclusion.

### 6.3.5 Computers create evidence as well as record and produce it

Traditional, paper-based account books consisted of sheets of paper onto which handwritten or typed entries were recorded manually; subsequent calculations were also substantially manual, even if a simple calculator was employed for some of the stages. But in the computerised equivalent, it is only the original entries that are input manually – all the other "records" are produced by the computer. There are many examples where computers "assemble" documents, etc. and only do so at the point at which a request is made for the document to be created. This can be true of online requests as well as conventional printouts or on-screen reports.

### 6.3.6 The changing ICT landscape

The ICT landscape of hardware, operating systems, software, application programs, communications protocols and social and commercial infrastructures is in constant change. The vast majority of "forensic science" deals with underlying physical, biological and chemical situations which do not change, although over time new techniques for analysing them emerge. But in ICT, significant changes are to be expected even over a five-year period. The Internet as a consumer "product" only dates from 1994/5. Specialists in digital forensics have to cope with an unparalleled rate of change but still strive to work to the same standards of rigorous verification that are expected in the more traditional forensic disciplines.

## 6.4 Cyber-evidence in Practice

Computer evidence can consist of, among other things:

- **content** – of a file, typically, the words and figures in a document or report, images, designs within an application file, a database or selection, emails, webpages, files downloaded;
- **meta-data** – within certain files, that is, data about data which is not immediately viewable but indicates, for example, who created a file, how many times it has been edited and when it was last printed. Microsoft word processing and spreadsheet documents may contain extensive meta-data;
- **directory data –** information about a file which is held in a system's storage media containing details of name, various associated date and time stamps, and size;
- **configuration data** – files and directory data which help a computer and/or application programs to behave in a particular way and which may provide evidence of how and when the computer was used. On a Windows PC, this includes material found in the registry;
- **logging data** – files created by application programs and operating systems which either record activity explicitly as in audit trails and online keystroke captures, or which can be used to attempt to reconstruct events, eg "history", "session" and "recent" files;
- **material from back-ups** – depending on the circumstances, any of the above;
- **forensically recovered data** – material obtained from storage media which would not normally be seen, eg undeleted files, files from slack space, swap files, caches, plus of fragments of any of the above;
- **eavesdropped data** – material obtained by placing a monitor across a telephone or network connection. This in turn divides into two:
  - traffic data – who called whom, when and for how long;
  - content – what was said;
- **expert interpretations** – based on any of the above in any combination.

These categories are not mutually exclusive.

## 6.5 Continuity of Digital Evidence

This encompasses the same underlying concepts as those for more physical types of evidence. Clearly, some types of “computer” evidence are physical objects – personal computers, disks, disk media, PDAs, mobile phones and so on – and these are bagged and tagged in the same way as the paraphernalia of street crime. Particular care may need to be taken with the storage conditions of computers, mobile phones and PDAs. Some gadgets need to be supplied with electrical power, or their internal clocks (even data) may fail. Some media may be spoiled by proximity to magnetic currents or damp.

Evidence which is in electronic format can be demonstrated to be uncontaminated if at an early stage it has been subjected to digital fingerprinting (MD5 and similar tests[11]) and the original digital fingerprint has compared successfully with the tendered exhibit.

But there is a further meaning to “continuity of digital evidence”: most exhibits produced to a court are *derived* from material originally acquired, not the material itself. Often, at the very least, it will be a printout of material originally found in digital form – there needs to be clear continuity on whether the printout is complete and reliable and who carried it out. To take the matter a little further: by itself an entire log file is indigestible; usually someone will have used software tools to look for patterns of activity that are thought to be significant. The same applies to any of the large databases that are usually at the heart of most commercial enterprise packages, which record orders received, goods despatched, send invoices and create a general ledger; it will only be selections from the database that are relevant. Again, a court is unlikely to be comfortable when presented with an entire PC; an analyst will have carried out searches for files and perhaps other patterns of usage. Continuity means that the defence team has to be in a position to trace back from the helpful *derived* evidence to the raw material from which it has been drawn. This is not only to ensure that the evidence has not been altered during processing, but also to establish that no mistakes have been made by the analyst or the tools deployed – and also for the defence to be able to argue that other selections and analyses may produce very different results.

[11] A file or an entire disk is subjected to a mathematical process to produce a “result”; in effect a short stream of letters and numbers. Once that file or disk has been copied the same mathematical process is re-applied and should produce the same “result”; if it doesn’t the copy is not identical to the original

# 7 Devising the Corporate Plan of Action

By now it should be possible to identify the elements in a corporate plan of action in order to be able to respond to the requirements of producing digital evidence. Table 7.1 (below) provides an outline. As with any generic list, some items will be inappropriate for certain types of organisation and larger types of business may need to add further elements. Small and medium-sized enterprises may feel that the list is more sophisticated than they require; although they may lack such things as a "disaster recovery team", nevertheless this is function that they need to anticipate. The table is divided into anticipatory measures, incident management measures and longer term measures. Some of the functions can be outsourced to third-party specialists – but careful decisions will need to be made about which functions and their extent. It should also be borne in mind that at any one time there may be several "incidents" in play, operating on a variety of timescales.

**Table 7.1: Outlining the corporate plan of action**

| **Anticipatory Measures** | |
|---|---|
| **Risk analysis** | The starting point is to identify the likely triggers for situations where evidence may be needed. These will include a number of the events almost certainly already identified during a conventional security risk analysis, but in addition should also include "lesser" events such as disputed transactions, employee disputes and breaches of contract (see Chapter 5: Risk Scenarios).<br>A "frequency of occurrence" estimate for each would help to set priorities. A "cost of occurrence" calculation will need to include direct, consequential and reputational losses. |
| **Desirable evidence analysis** | For each event identified a list of potential desirable sources of evidence should be produced. |
| **Available evidence review** | The analysis should then be compared with what is actually available and deficiencies identified. |
| **Assembly of key system documentation** | In any unexpected event it is often helpful to have at hand key system documentation so that additional potential sources of evidence can be identified or additional monitoring introduced. The documentation may assist in explaining aspects of the system and services to third parties, such as investigators and the legal system. |
| **Review of back-up, archiving procedures and facilities** | Computer-dependent organisations usually only back up for the purposes of disaster recovery or regulatory compliance. But good back-up may also provide good evidence. |
| **Evidence collection and preservation policy and specific guides** | At this point it should be possible to produce a written policy for evidence collection and preservation, plus a series of specific guides to cover particular computer resources. The guides should have a similar status to disaster recovery plans, and be subject to periodic revision and testing. |
| **Set up incident management team** | It has to be clear who is supposed to do what and to whom they report. An incident management team will require resources (see below). |

| | |
|---|---|
| **Review of employment contracts, etc.** | The organisation may need certain additional powers to remove any ambiguity about its right to collect certain kinds of evidence as there is the potential for clashes with, for example, human rights and data protection legislation. Adjustments in contracts of employment and notifications regarding changes of policy may be necessary. |
| **Identification of gaps** | The above exercises will probably result in the identification of gaps in response. The urgent issues (defined from the risk analysis) will need swift attention; longer term matters can be put into a future programme. |
| **Incident management measures** | |
| **Reporting point/first responder and procedures** | This is the person or team to whom suspicions and fears or requirements to produce evidence are first reported. In an incident, this is the individual who will make the initial diagnosis.<br>Every member of the organisation should be clear about who reports should be made to. Those who receive such reports should have, among other things, excellent sober diagnostic skills. Quite often, initial fears may be exaggerated and all that is required is that information technology (IT) support is brought in for a remedy. |
| **Incident management team** | One of the key lessons from conventional disaster recovery management is that the main board of an organisation should not attempt the detail of response but, while maintaining supervision and ensuring adequacy of reporting, should delegate the task to a specialist team.<br>Helpful advice about Computer Security Incident Response Teams (CSIRTs) can be found at http://www.cert.org/archive/pdf/03tr001.pdf. Depending on the circumstances, this team may have strong links with existing security and contingency planning teams, although the emphasis may need to change. A typical team might include:<br>• the head of IT;<br>• the head of IT security;<br>• links to the board/chief executive (if not already arranged);<br>• a representative from corporate security;<br>• a representative from human resources;<br>• a representative from public relations;<br>• a lawyer (internal or external);<br>• a leader of specialist investigators/technicians (internal or external). |
| **Role of top management** | By implication, the role of the main management team may have, in addition to their regular duties, the following additional ones:<br>• supervision of the emergency management team, including specific tasking, resourcing, performance;<br>• assessment of diagnoses;<br>• review of the implications for main business activities;<br>• review of the implications for relationships with customers, bankers, the investment community, etc.;<br>• review of any specific legal requirements and regulatory obligations thought to be at risk;<br>• review of implications for employees and contractees, including the possibility of termination;<br>• consideration of the need to report suspected crimes to the authorities, the nature of liaison;<br>• supervision of insurance claims and asset recovery;<br>• supervision of public relations issues. |
| **Resourcing – internal** | A tempting option is to consider having in-house forensic computing expertise. There will probably be no shortage of techies who would love |

|  |  |
|---|---|
|  | to attend courses and buy appropriate kit. Specialist vendors who have concentrated mostly on law enforcement are now expanding their products into the corporate market.<br>The problem for many individual organisations is that for most of the time they will have no need for forensic computing skills, but when they do, they may need very high levels of skill, and may also want it in quantity. Perhaps the best analogy is that of medical First Aid: all organisations of any size need a competent First Aider, some may be so large as to justify the employment of a few nurses and perhaps even a doctor. But very few need a permanently-employed surgeon. Thus, for most organisations, what is likely to be required is someone with a basic awareness of evidence collection issues and a knowledge of what specialist third-party suppliers can offer. |
| **Resourcing – third-party contracts** | If specialist skills are going to be required from third parties – and more often than not for most organisations this will be the case – it is better to know where they are going to come from and not rely simply on advertisements. Will the organisation need consultants for high-level strategic advice, good contacts with law enforcement and the regulatory authorities, investigatory skills or detailed technical support, and in what combinations?<br>In terms of likely need, a review of the firms and individuals that are available, as well as their strengths and weaknesses, is essential. As with any purchase of third-party security services it is important to establish that the company has relevant experience (as opposed to simply having an impressive background in law enforcement or intelligence) and that it is trustworthy.<br>It may be useful to contemplate a contract for services on a contingency basis: this enables the parties to evaluate each other and for the supplier company to have sufficient pre-knowledge of an organisation's IT infrastructure and internal culture to be able to respond promptly. |
| **Asset recovery, loss mitigation issues** | During any incident where there has been a loss, whether tangible or reputational, the organisation will want to have specific resources for recovering assets and minimising/mitigating other losses. This is a normal security function. The existence of good-quality evidence of the types and quantum of loss will assist. |
| **Legal and law enforcement liaison** | At a practical level it is important to designate a Single Point of Contact (SPOC) to deal with law enforcement requirements. This enables an organisation to track every contact with law enforcement and also simplifies the tasks of law enforcement investigators. The function is distinct from the role of a legal adviser – the SPOC will need to mediate and serve law enforcement and prosecutor requirements for access to specific evidence, background information and arrangements to interview individuals.<br>The SPOC should be able to respond to requests for formal disclosure. Later, they may need to make arrangements for court appearances. In a civil case involving complex evidence, a technically-aware SPOC will be required to deal with lawyers and the needs of specialist expert witnesses (on both sides). The task of SPOC could be combined with that of first responder, as overlapping skill sets are required. |
| **Longer term measures** |  |

| | |
|---|---|
| **Programmes to address gaps in available evidence** | Faced with the many issues surrounding provision of reliable digital evidence, most organisations will aim for an initial programme to meet the most urgent and obvious needs.<br>Once this task has been achieved, any plan should be subject to periodic review and revision.  Business functions and technical infrastructures tend to change significantly over time; in addition, new forms of IT-related crime become fashionable, causing a change in the requirements to produce evidence. |
| **Improvements in overall system specification and management procedures to capture more potential worthwhile evidence** | |
| **Improved enhanced local evidence handling training** | |

## 8 Issues for the Future

A little over ten years ago the commercial, retail Internet was just beginning. There was almost no Internet-based e-commerce, no Internet-based e-banking, Google, Amazon and other commercial giants of cyberspace scarcely existed. Typical PCs had hard disks with capacities measured in megabytes, not gigabytes, and the Microsoft Windows family of operating systems was launched in 1995. Email was possible but existed in a series of silos dependent on the employer, or the "community" to which a person belonged, not as a universal standard. Even those relatively few UK homes that connected digitally to the outside world used dial-up – always-on broadband was a dream for the far future. By 2006 69% of all UK Internet connections were broadband and over 57% of all UK homes had Internet access. 70% of UK businesses had a website, 15% sold over the Internet and nearly 60% bought over the Internet. Five years ago, digital cameras were an expensive gimmick and had specifications less good than those found in many of 2008's mobile phones. The hard disk-based miniaturised portable music and media player has been around since 2003 but capacities and facilities have increased prodigiously.

Costs continue to fall. Laptops with large hard-disks and the most recent operating systems now cost less than £300, which translates to less than 3 days' earnings for a semi-skilled painter/decorator in London, 5 hours of the time of a skilled plumber and perhaps 40 minutes with a partner at a leading solicitors' firm. External hard-disks, a key risk factor in data theft, cost under 12p per 1000 MB of storage. Just before Easter 2008 you could buy an easily-secretable 8 GB USB thumb drive for under £15. For £15/month you could also get fully mobile Internet on your laptop and with 3GB download per month – and the hardware dongle to do so was free.

It is obvious that these technological changes have brought about profound changes in everyday private and commercial life. And almost every one of them has created opportunities for new forms of crime, albeit often variants on existing ones. Ten years ago, almost no one was predicting a crisis for the music and film publishing industries prompted by easy, low-cost copying and distribution of their product. And only the very paranoid were predicting the extent to which individuals might leave large numbers of digital footprints of their activities. Ten years ago mobile phones simply made and received telephone calls, today they are fully fledged computers capable of connecting to the Internet, handling emails, storing and generating substantive work files, photographing still and movie pictures, and playing music and video files. The mid-2000s saw the growth of social networking sites. In one sense social networking has been around for a very long time: the Bulletin Board Systems of the early 1980s, well before the arrival of the Internet, provided a medium in which people could meet. What the likes of Facebook, Bebo, LinkedIn and their siblings have provided is a much richer, more fluid and easier to use mechanism. But their very popularity has made it much easier for investigators to identify private detail about individuals which can later be exploited.

For organisations and individuals that recognise the need to be able to capture digital evidence of important transactions and activities, the lesson is: today, whatever analysis you carry out and whatever measures you install, they will become rapidly obsolete.  No longer on the horizon but arguably already with us are ever-expanding amounts of personally-created data, ever higher speeds of data transfer, always-on portable computing, cloud computing, ubiquitous computing, remotely-located data stores protected by strong encryption and grid computing.

It would be a rash futurologist who made predictions at too great a level of detail. And that includes forecasts of how digital forensics might have to respond.

## Appendix 1: Preservation of Evidence – Guidelines

The only area where there are well-developed procedures for seizing digital evidence relates to data on hard disk – disk forensics – where a number of organisations have published guides[12]. Many of them are similar to the *Good Practice Guide* of the UK's Association of Chief Police Officers (ACPO)[13], which has some useful principles.

> Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
>
> Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
>
> Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The Guide goes on:

> Computer-based electronic evidence is no different from text contained within a document. For this reason, the evidence is subject to the same rules and laws that apply to documentary evidence.
>
> The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of the police.
>
> Operating systems and other programs frequently alter and add to the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.
>
> In order to comply with the principles of computer-based electronic evidence, wherever practicable, an image should be made of the entire target device. Partial or selective file copying may be considered as an alternative in certain circumstances e.g. when the amount of data to be imaged makes this impracticable.

[12] See below.

[13] Available at: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf; http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

> In a minority of cases, it may not be possible to obtain an image using a recognised imaging device. In these circumstances, it may become necessary for the original machine to be accessed to recover the evidence. With this in mind, it is essential that a witness who is competent to give evidence to a court of law makes any such access.
>
> It is essential to show objectively to a court both continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

A proposed Standards for the Exchange of Digital Evidence from the International Organisation on Computer Evidence suggests a similar set of principles for the standardised recovery of computer-based evidence[14]:

- upon seizing digital evidence, the actions taken should not change that evidence;
- when it is necessary for a person to access original digital evidence, that person must be forensically competent;
- all activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved and available for review;
- an individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession;
- any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

The US Department of Justice Guidelines can be found at:

http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm

### *Council of Europe Cybercrime Convention*

The Council of Europe Convention on Cybercrime of 23 November 2001 is the first internationally binding legal instrument with regard to the consequences of modern information technology for criminal law and procedure. Although the Council of Europe is a regional body, the Convention provides for a global framework for law enforcement in cyberspace; non-Member States of the Council of Europe such as Canada, Japan and the US contributed to the preparation of the Convention and

[14] For a G8 conference: http://www.ioce.org/G8_proposed_principles_for_forensic_evidence.html

accordingly signed and supported the agreement[15]. The Convention aims to provide harmonised definitions of various computer-related crimes, so that mutual cooperation and extradition can be expedited. Most jurisdictions require some equivalence between their own law and that of the country requesting assistance before they will grant an extradition request.

The Convention also extends towards issues involving evidence, both in terms of warranting methods and actual procedures. With regard to electronic evidence, Council of Europe Recommendation No. R(95)13 concerning problems of criminal procedural law connected with information technology[16], adopted on 11 September 1995, states the following:

> Special procedures and technical methods for handling electronic evidence should be developed which ensure and reflect the integrity and authenticity of the evidence. Legal provisions on evidence relating to traditional (paper) documents should similarly apply to electronic documents. (Principle IV.13)

The Explanatory Memorandum to the Recommendation explains the difficulties of electronic evidence as opposed to paper documents:

> Among other things electronic documents can only be read by means of special hard- and software and they can be easily manipulated in such a way that the manipulation is not detectable by the eye. (Para. 152f)

The Explanatory Memorandum suggests different procedures for authentication of electronic evidence, as with the establishment of a complete chain of custody, from the person who first copied the data to the person who produced the printout for the trial, or the use of electronic signatures (para. 161).

The development of a harmonised approach in this matter at an international level is indispensable because IT offences are often cross-border in nature (para. 164). Otherwise, according to the Explanatory Memorandum, serious problems with regard to the admissibility of electronic evidence will continue to exist. (ISO 15489, the International Standard on Records Management, discussed below).

[15] Chart of signatures and ratification of the Convention on Cybercrime: http://conventions.coe.int/ Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=09/07/04&CL=ENG. The Convention on Cybercrime entered into force on 1 July 2004.

[16] Available at: http://www.coe.fr/cm/ta/rec/1995/95r13.htm

Table A.1 notes some of the more important standards and initiatives.

**Table A.1: Standards and initiatives**

| | |
|---|---|
| **ACPO** | The *Good Practice Guide for Computer Based Evidence* is available for download from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.<br>It is fair to say that its main focus is on disk forensics, PDAs and mobile phones as opposed to larger computers and networks but there are some useful general principles, an overview of legal issues, a glossary and a list of UK police contact points |
| **US Department of Justice** | The Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, of the US Department of Justice provides a useful manual, available at: http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm and http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm<br>Obviously, the description of the law is for US readers. The overall CCIPS site contains many documents, press releases and links of considerable value to the researcher: http://www.usdoj.gov/criminal/cybercrime/<br>and contains references to the Council of Europe Cybercrime Treaty to which the UK is a signatory. There is also a *Guide for First Responders*: http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf |
| **Council of Europe Convention on Cybercrime** | The Convention aims to harmonise definitions of cybercrime and procedures for warrants and evidence collection across international jurisdictions. It provides significant guidance on evidential standards. http://www.coe.fr/cm/ta/rec/1995/95r13.htm |
| **Scientific Working Group on Digital Evidence (SWGDE)**<br>**International Organisation on Digital Evidence (IOCE)** | SWGDE was established in February 1998 through a collaborative effort of the Federal Crime Laboratory Directors.<br>http://www.swde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf<br>As the US-based component of standardisation efforts conducted by the IOCE, SWGDE was charged with the development of cross-disciplinary guidelines and standards for the recovery, preservation and examination of digital evidence, including audio, imaging and electronic devices: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm |
| **Internet Request for Comments (RFC)** | Internet RFC 3227 provides the *Guidelines for Evidence Collection and Archiving* (http://www.faqs.org/rfcs/rfc3227.html). RFCs are one very important way in which Internet protocols and good practice are discussed and promulgated: http://www.ietf.org/rfc/rfc3227.txt |
| **(Cyber Tools Online Search for Evidence) CTOSE** | CTOSE was a research project funded by the European Commission. Its purpose was to gather available knowledge from different expert groups on all the processes involved in dealing with electronic evidence and to create a methodology on how to deal with electronic evidence that might occur as a result of disputed electronic transactions or other computer related and hi-tech crime: http://www.ctose.org/ |

| | |
|---|---|
| **ISO 17799 / ISO27001** | ISO 17799 and now IS27001 is the International Standard for Information Security Management. It addresses many aspects of information security and internal controls, but also stresses the need for formal incident response procedures and tools. These procedures should cover:<br>• analysis and identification of the cause of the incident;<br>• planning and implementation or remedies to prevent recurrence, if necessary;<br>• collection of audit trails and similar evidence;<br>• communication with those affected by, or involved with, recovery from the incident;<br>• reporting the action to the appropriate authority.<br>The organisation that has suffered a security incident must collect evidence properly for three purposes:<br>• internal problem analysis;<br>• use as evidence in relation to a potential breach of contract, breach or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;<br>• negotiating for compensation from software and service suppliers.<br>See: http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35 |
| **ISO 15489/ British Standards Institute PD0008** | International Standard on Records Management – standards for record-keeping in electronic form<br>http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31908&ICS1=1 |
| **Handbook of Legal Procedures of Computer and Network Misuse in EU Countries** | 2005 Project to update the EC Handbook of Legislative Procedures of Computer and Network Misuse. It will include a confirmation and review of the existing information, as well as collection of legislative information relating to the 10 new member states.<br>http://www.csirt-handbook.org.uk |

## Appendix 2: Preservation of Evidence – Individual Procedures

### *Individual Workstations/Personal Computers*

The aim is to make an exact copy of the hard disk(s) as soon as possible after the computer has been seized. The exact copy must include not only all the normally visible files but encompass all the sectors of the hard disk, even if initially they appear to be empty, so that any deleted data fragments can be recovered. Technicians and investigators must avoid contaminating the evidence so that what is produced is a detailed snapshot immediately prior to seizure. The process is called "forensic imaging".

To be carried out successfully this requires both appropriate technical products and following certain procedures. Each step in turn needs to be carefully recorded so that there is no opportunity for others to question the technician's skills.

There are a variety of software products. Retail "imaging" products are designed to assist recovery after a hard disk failure. For PC, products such as Ghost, Acronis True Image, Paragon and Powerquest DriveImage (for Apple Mac, SubRosaSoft's CopyCatX II) may not be adequate in a forensic arena as they usually concentrate only on "live" files as opposed to data that has been deleted but are still resident on disk; some retail imaging products actually add data during imaging. *dd* is a reliable and flexible standard part of Unix operating systems and is completely free, although not easy to use. Most computer forensic practitioners use stand-alone products such as SafeBack, EnCase or FTK Imager. The latter two provide a complete disk forensics suite, including imaging. The professional products often contain in-built integrity checking, so that an "image file" (intermediate file which either can be directly examined or from which exact clones of the original can be made) can be verified against the original using "digital fingerprinting".[17] Not all imaging products can cope with all the disk operating systems that might be encountered and some versions of well-known products may fail to capture everything on a hard disk, which is why competent technicians need to be employed to carry out the work.

The first task is to ensure that, once the computer has been seized, the computer is not booted up normally as, under most modern operating systems, during the process fresh data will be written to disk, even if all that happens is that the computer is started up and then almost immediately afterwards shut down. To avoid this, usually a technician will remove the hard disk and install it in his own specialist workstation. The workstation will contain, among other things, specialist "imaging" software; a write-protect device so that the hard disk to be imaged can only be "read", not "written to"; and a further hard disk onto which the resulting "image file" can be stored prior to being backed-up to DVD and/or CD, tape or network store. In the case of a laptop or other computer where disk removal is difficult, the computer is started up with an alternative operating system from the CD drive. The special CD contains the imaging software and networking capability. The computer to be imaged is linked via a network or parallel cable to the technician's computer, which then takes charge of events and collects the image file over the network cable. (The network actually

[17] A complex mathematical calculation is performed on the contents of the original and then on the clone – if original and clone are identical, the product of the calculation will also be identical.

consists of only two computers and the cable has to be of the “cross-over” variety). “Network” imaging tends to be a lengthy process because of the slow speed of data along the cable compared with carrying it out disk-to-disk; “parallel port” acquisition takes even longer and is of course impossible on more modern computers where serial and parallel interfaces have been replaced with USB ports .

There are also specialist hand-held hardware devices which can carry out high-speed imaging of disks, once they have been removed from their computers. They are of particular value when time is of the essence, for example where computer downtime may incur extensive consequential loss.

In general terms, a PC that is seized in depowered mode should not be started up by anyone other than by a trained forensic technician. PCs that have to be seized while powered up will require careful consideration to decide the precise method; if the suspect is an ordinary user, a note of what is on screen and perhaps photographs of the screen, plus notes and photographs covering all cables, etc. connected to the PC is often sufficient. If the suspect is an IT specialist, where there is the possibility that “logic bombs” are already in place to destroy data wholly or partly, or where there may be a link open to a significant remote computer, then it is essential to involve a trained forensic technician before any attempted seizure takes place, as there may be a variety of opportunities to capture essential evidence and avoid data destruction.

A further problem occurs where a larger “personal” computer contains several hard disks designed to work together in a “RAID” array. These are used mainly where very fast performance is required, as in an office server or in video-editing workstations. Usually, the disks cannot be imaged separately and specialist assistance is required to determine the best course of action.

In any event, the technician will make contemporaneous notes of what has been done, to be incorporated in a witness statement or exhibit later.

A further essential task for the technician is to check the “clock-time” on the computer that is being imaged. All computers have an onboard clock, sometimes referred to as the BIOS clock, from which the day and time stamps used by the computer are derived. It is important to establish how far the computer’s clock-time diverges from the actual time, as this may have an impact on assessments of chronologies of events later. A handy tip is to get the computer’s BIOS screen to a point where the clock is visible and then to place next to it a clock which takes its timing from an “atomic” source; the two are then photographed together using a digital camera or cellphone with in-built camera.

Some software-based imaging products permit the technician to “preview” a hard disk of interest – that is, carry out an initial examination safely but without first having to make an image. This can save time by the early elimination of “irrelevant” material and is particularly useful when large numbers of disks have to be examined.

Most of the popular forensic analysis products available are for PCs running the Windows family of operating systems.[18] Examples include EnCase[19], AccessData

[18] Many of these do much more than preserve evidence – they also perform analyses

FTK[20] and ProDiscover[21]. Many of these products can also cope with Linux and some other Unix family operating systems. However, experienced forensic technicians often prefer to use Linux-based forensic tools to examine Linux-based hard disks. Examples include SMART[22] and Sleuthkit[23]. The Apple Mac family is relatively poorly supported by commercial forensic tools. EnCase "understands" the disk filing system, but there are now specialist tools such as SubRosaSoft's MacForensics Lab[24] and the Black Bag suite[25]. Since Apple OS X is in fact underpinned by BSD Unix, it is possible to use Unix-based tools for imaging and analysis.[26]

If a hard disk of any kind is found to be of interest, it should be properly sealed as a potential exhibit. If the owner of the original computer says that the hard disk contained essential working data, a clone of the hard disk can be made from the original onto a new hard disk which can then be installed in the computer; alternatively, key files can be exported to CD, DVD or external hard disk. Hard disks are now extremely low-cost and there is little excuse for not preserving original evidence. There may be circumstances in which some of the material found on a hard disk is such that it should not be returned to general circulation. Examples include indecent images, data subject to the Official Secrets Act and terrorism legislation and material which might prejudice a fair trial. In these circumstances it will be necessary to negotiate with the law enforcement agency for the release of essential but non-sensitive material.

### *Legal issues*

Seized computers will normally be regarded as "real" evidence for admissibility purposes. However, the contents of individual documents (files) found on a computer may need to be admitted separately[27], particularly if more than one person has had routine access to that computer. Investigators also need to demonstrate that they are "authorised" to access the computers for the purposes of the Computer Misuse Act 1990.

In general terms, employers and their agents are normally "authorised" to access computers used by their employees, but this may be subject to a detailed examination of contracts of employment. Section 10 of the Computer Misuse Act 1990 protects law enforcement officers in the execution of their powers of inspection, search or seizure. Where computers are seized from professionals such as lawyers and accountants there may be issues of professional privilege (under Part 2 of the Criminal Justice and Police Act 2001 and associated codes of practice)[28]. Section 54 restates

[19] http://www.guidancesoftware.com/

[20] http://www.accessdata.com/products/ftk/

[21] http://www.prodiscover.com/ProDiscoverDFT.htm

[22] http://www.asrdata.com/tools/

[23] http://www.sleuthkit.org/

[24] http://www.macforensicslab.com/

[25] http://www.blackbagtech.com/software_mfs.html

[26] Newer Macs powered by Intel chips also have a replacement for the BIOS called EFI (Extensible Firmware Interface) which in turn affects how the computer boots up and hard-disks are partitioned; older forensic analysis tools can only "see" the contents of such hard-disks after manual fiddling,

[27] For example, under the business records provisions in s. 117 of the Criminal Justice Act 2003.

[28] Actually an update of the Police and Criminal Evidence Act 1984, Code B.

the rule that legally privileged material seized in a warrant must be returned. But it goes on to say that legally privileged material can be retained if it is “inextricably linked” to other material which is seizable.

## *Evidence from Keyloggers*

A keylogger is an item of hardware or a covert software program which, as the name implies, captures every keystroke made on a computer such that the activities of the user can be reconstructed. Hardware versions are usually inserted between the keyboard and the computer and are normally so physically small that only careful inspection will reveal their existence. Keyboards are normally connected to computers via a PS/2 or USB interface; keyloggers are available in both formats. The keyloggers have memory storage facilities and the investigator periodically collects the data and plays it back on his own computer. Some keyloggers can also capture whole screens.

Software versions offer similar facilities and are usually designed to operate covertly – their existence is not shown up when a computer user tries to find which programs are “running” on his machine. Software keyloggers, once installed, can usually be controlled remotely, across a network or the Internet, provided of course that the targeted computer is actually connected to a network. Most software keyloggers can be asked to perform screen-captures, or send messages to investigators if particular keywords are triggered.

### *Legal issues*

Assuming for the moment that the keylogger is being installed by an investigator instructed by the employer of a suspect, the legal considerations are similar to those for any other sort of employer-based investigation. These are covered in Appendix IV. In other circumstances, the use of software-based keyloggers involves breach of s 3 of the Computer Misuse Act 1990. Hardware-based keyloggers might, it could be argued, be counted as “interception” for the purposes of s 1 of the Regulation of Investigatory Powers Act, 2000.

## *Large and Medium Computer Systems*

Traditionally, the courts have simply accepted the printout of reports and documents. In the UK police powers to obtain these in the course of a search are covered, among other places, under general powers of seizure in s. 19 of the Police and Criminal Evidence Act 1984. Section 19(4) permits “the constable” to require that information held in a computer is “to be produced in a form in which it can be taken away and in which it is visible and legible”.

But should an organisation not now be expecting the system to be “imaged” in the way that it is for single hard disks, so that defence experts are absolutely sure that they can run as many verification tests as they wish? Does an organisation have to make a forensic copy of the entire network of a large bank with a global presence and all its subsidiaries, just because an assistant manager in a UK branch is accused of fraud by colluding with customers over credit agreements and says that the computer is not accurately reflecting all the business transactions and queries made?

Often, it is not feasible to "image" or "clone" larger computer systems, so some form of selection will have to be made. In so doing, several things need to be borne in mind:

- the organisation needs to persuade a court that the output of the computer, taken as a whole, is reliable;
- the organisation has to show that it has captured the "complete" evidence in terms of the litigation being pursued, not just a selection favourable to its case;
- the evidence must be admissible.

In terms of the overall reliability of a computer system, the following elements in a witness statement may help to persuade a sceptical court:

- a description of the computer system's overall functions within the organisation;
- an account of how long the system in its present configuration has been in operation;
- what forms of testing took place prior to commissioning and what forms of routine audit are in place;
- what external factors exist to act as a check on reliability. For example, most accounts systems refer to transactions with other organisations and banks – failures in an organisation's own computer systems would soon produce complaints from counterparties. Third-party computer records may corroborate the records an organisation wishes to introduce in evidence;
- what security features exist and how they are managed – this is to anticipate a suggestion that incriminating material was placed there by someone other than the suspect;

In terms of the exhibit that is being produced, it is useful to be able to give the following:

- where it comes from:
    - o is it in the form of a report that the computer regularly produces as part of its normal functions?
    - o is it a regular audit or log file generated as part of the computer system's normal functions?
    - o is it a regular back-up – if so, how far is it a "complete" back-up?
    - o if the exhibit is the result of monitoring or specialised analysis to test initial suspicions, how was the monitoring set up?
- how the selection of evidence was made and why it can be regarded as "complete" in terms of the issues at hand;
- what procedures were used to collect the evidence such that it can be regarded as free from tampering;
- what procedures were used to preserve the evidence so that it can be regarded as free from subsequent tampering. This may take the form of imaging some computers or copying selected files to write-once data media such as CD or DVD, or making a digital fingerprint of the files;
- what manipulation or subsequent analysis was carried out to make the material "easier to understand" – this is a perfectly legitimate course of action, but in this event the original material should be exhibited so that the defence team can test the manipulation or analysis.

An organisation should be prepared for defence team demands for further disclosure so that they can test the overall reliability of its evidence and perhaps request further information from its computer system in order to test or prove assertions of their own.

*Legal Issues*

Usually, admissibility of evidence will be on the basis that the material is a "business record" as defined in s. 117 of the Criminal Justice Act 2003; an "expert report" for the purposes of s. 118(8) and 127 of the same Act; or "real evidence". However, evidence may be excluded, for example if it has been obtained unfairly (judicial discretion under s. 78 of the Police and Criminal Evidence Act 1984), or in contravention of data protection or human rights legislation.

## *Corporate Networks*

In addition, often it is not feasible to "image" or "clone" networks. Apart from the quantity of machines that would need to be imaged, if the evidence is to have real integrity, the entire network would have to go offline and be shut down for the duration. If this does not happen, then the images of each of the various constituent computers will be "snapshots" taken at different times – the data will not synchronise and corroborate. So, again, the form of selection will have to be made. In so doing, several things need to be borne in mind:

- the organisation needs to show that it has captured the "complete" evidence in terms of the litigation that it is pursuing;
- the evidence must be admissible.

An organisation will need to be able to justify the overall reliability of the network and the particular workstations and servers that it is submitting as evidence. The following elements in a witness statement may help to persuade a sceptical court:

- a description of the network's overall functions within the organisation;
- the network's topography – does it have one server, several servers or none? Are there any unusual features about the communications links?
- how the network is managed;
- what security features exist and how they are managed – this is to anticipate suggestion that incriminating material was placed there by someone other than the suspect;
- how long the network in its present configuration has been in operation;
- what forms of testing took place prior to commissioning and what forms of routine audit are in place;
- what external factors exist to act as a check on reliability. For example, most accounts systems refer to transactions with other organisations and with banks – failures in a business's own computer systems would soon produce complaints from counterparties; third-party computer records may corroborate the records you wish to introduce in evidence;
- what can be said about the reliability of the constituent elements of the network – operating systems, software, hardware;
- compliance with any external good practice or system audit standards.

In terms of the exhibit that is being produced, it is useful to be able to say:

- where it comes from:
  - is it in the form of a report that the system regularly produces as part of its normal functions?
  - is it a regular audit or log file generated as part of the normal functions?
  - is it a regular back-up – if so, how far is it a "complete" back-up?
  - if the exhibit is the result of monitoring or specialised analysis to test initial suspicions, how was the monitoring set up?
  - is a complete image being provided of key workstations and servers?
- how the selection of evidence was made and why it can be regarded as "complete" in terms of the issues at hand – why it was considered safe to exclude other potential sources of evidence? Particular regard should be given to the position of servers;
- what procedures were used to collect the evidence such that it can be regarded as free from tampering;
- what procedures were used to preserve the evidence so that it can be regarded as free from subsequent tampering. This may take the form of imaging some computers or copying selected files to write-once data media such as CD or DVD, or making a digital fingerprint of the files;
- what manipulation or subsequent analysis was carried out to make the material "easier to understand" – this is a perfectly legitimate course of action, but in this event the original material should be exhibited so that the defence team can test the manipulation or analysis.

As always, an organisation should be prepared for defence team demands for further disclosure so that they can test the overall reliability of its log evidence and perhaps request further information from its computer system in order to test or prove assertions of their own.

In the last few years products have begun to emerge which allow for workstations to be remotely monitored and imaged across a corporate network. The most mature products appear to be EnCase Enterprise Edition and ProDiscover Professional. These new products require that each workstation to be monitored has a small "servelet" program installed on it. The monitoring takes place from a specially designated workstation and the servelet on each monitored workstation accepts commands from it. Communications between the monitoring and monitored workstation run across the corporate network, but are encrypted. The hard disk on the monitored workstation becomes "write-protected", just as it would during a conventional examination, so that the process should be free from contamination by the examiner.

Although this approach seems very promising it has yet to be tested fully in the courts and there may be practical problems such as the time taken to image. For any organisation considering the deployment of remote monitoring or imaging, in addition to the costs of the software licence, significant funds will need to be set aside for the related training and development of appropriate procedures. There will still be problems of selection of material and anticipating how a defence expert might test it – or the defence team complaining that their expert is not able to conduct a realistic test and that as a result the evidence should be excluded.

Admissibility of evidence will be on a similar basis to that for material obtained from large computer systems: that the material is a "business record" as defined in is a "business record" as defined in s. 117 of the Criminal Justice Act 2003; an "expert report" for the purposes of s. 118(8) and 127 of the same Act; or "real evidence". However, evidence may be excluded, for example if it has been obtained unfairly (judicial discretion under s. 78 of the Police and Criminal Evidence Act 1984), or in contravention of data protection or human rights legislation.

Where remote monitoring has been used, there may be arguments which suggest that a interception for the purposes of the Regulation of Investigatory Powers Act 2000 has taken place. Employers should be able to have the benefit of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[29]. This allows a business to carry out an interception on its own network in order to: "establish the existence of facts", "in the interests of national security", "for the purpose of preventing or detecting crime", and "for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system". In any event, in a corporate environment employees will need to be have been forewarned that their computer use may be subject to monitoring of various kinds.

## *Email*

Copies of emails may be found on the personal computers of the sender and the recipient and on one or more email servers. For each of these, copies may exist in archived back-ups. If either the sender or recipient uses a mobile device such as a mobile phone or PDA, copies may exist there as well. Obviously, a simple printout of an email is better than nothing, but because of the ease with which a wordprocessor can be deployed to alter or fake an email, a more sophisticated approach is required.

The key to securing reliable email evidence within an organisation is to know how the specific email service works – in particular, where copies of emails are likely to be stored. It is not unusual for suspects to attempt to delete emails from their local machine – hence the importance of being able to locate alternative copies. Clearly, each further copy of an individual email that is discovered provides greater levels of corroboration, and hence authenticity.

Emails sent over the Internet or using internet-like protocols have "headers" associated with them, which are normally suppressed when viewed through a regular email client program[30], which contain information about where the email originated and what route it took to the recipient. This information, though it can be forged or spoofed, can be used to provide a level of authentication.

[29] http://www.opsi.gov.uk/si/si2000/20002699.htm

[30] In Microsoft Outlook Express, for example, the headers can be viewed via right-clicking and selecting "Properties".

Email programs can be divided into two types: client programs, which are found on the PCs of those who send and receive email; and server programs, which act as a hub for email exchange between individuals within a business and also mediate the relationship with the outside world. Client programs include Microsoft Outlook and Outlook Express, Eudora and Thunderbird. Server programs include Microsoft Exchange, FTGate, MailTraq and IBM/Lotus Notes (although this last has a number of additional functions).

The emails themselves are stored in files associated with the email application – a forensic technician needs to have a knowledge of which files are important and where they are located. Attachments to emails may be stored elsewhere, in another directory on the disk. In the simpler older products, often the email files can be read directly using a text editor, but in more modern products such as Outlook and Outlook Express, the emails are held inside a structured database and can be read only from within the email program or a specialist utility. Email server programs also store messages within specialist databases. The advantage of the structured database is that it then becomes easy to carry out sophisticated searches for individual emails, by sender, recipient, subject, content, date and so on. In addition, the fact that each email is within a structured database makes tampering with the content of individual emails more difficult.

One disadvantage is that the set of emails within a database may contain material that is wholly irrelevant to the litigation and which is subject to data protection or human rights legislation, is commercially sensitive or covered by legal privilege. In these circumstances it may be necessary to arrange for an independent third party to have formal supervision of the files, along the lines of what is done in civil search orders or under Part 2 of the Criminal Justice and Police Act 2001 and associated codes of practice.

Some email services are presented via a web interface. For individuals, there are services such as Hotmail, Yahoo and Gmail, and many large ISPs offer a web-based service so that their customers can access email when away from their usual base via someone else's computer or an Internet café. Similar web-based email services can be offered by large organisations for their staff based on corporate email servers – Microsoft Exchange can be set up in this way, for example. In those circumstances the participants' PCs will not maintain a permanent record of emails sent and received. However, for recent emails, a computer forensic technician may be able to retrieve copies from the "temporary internet files" folders (also known as the cache).

### *Legal Issues*

There are some general restrictions on employer surveillance of employees and these apply to emails, phone calls and web browsing, among others (they also apply to the use of closed circuit television) (these are considered in Appendix 4).

Once these hurdles have been overcome, emails obtained from a PC may be admissible either as "business records" or as "real evidence" but there has to be a basis for them to be lawfully obtained in the first place. As far as PCs are concerned, the computer owner or another authorised person has to give permission, otherwise there may be an offence under the Computer Misuse Act 1990[31]. Further, this would produce the inevitable argument that information obtained in an unauthorised fashion should be excluded under s. 78 of the Police and Criminal Evidence Act 1984. It is likely that emails obtained from servers will be admissible as “business records”. However, if the server contains emails which have yet to be delivered to their destination, those emails might be regarded as still passing through a communications medium and thus be subject to the Regulation of Investigatory Powers Act 2000. So, part of the skill of looking for email evidence is to avoid those potential sources of emails which might be rendered inadmissible.

Statements producing email exhibits will need to cover the following:

- where the email has come from a client program installed on an individual PC – the identification of the program and the steps taken to capture and preserve the supporting files;
- where the email has come from a server program – the identification of the program and the steps taken to extract and preserve the supporting files; whether this is simply a subset of the total email data available and what basis was made for the selection, whether a larger subset is available against appropriate defence team request;
- in the case of a server program – what security features exist and how they are managed (this is to anticipate a suggestion that incriminating material was placed there by someone other than the suspect);
- compliance with any external good practice or system audit standards.

## *Personal Digital Assistants*

Despite their small physical size, PDAs are often substantial PCs in their own right. They hold personal data, diaries, documents and often emails. Increasingly, cellular phones and PDAs are converging.

In terms of capturing evidence, there are a number of choices. Ideally, like hard disks PDAs should be “imaged”. As with evidence from hard disks and other data storage media, it is important to be able to demonstrate that the process of collection has not caused the data to be modified. Just as with conventional PCs, in some instances the mere act of “just having a look” may cause data alteration. PDAs often contain two sorts of memory: internal and external. The external is usually on a card – Compact Flash, Secure Digital, etc., and this presents relatively few problems as the cards can be removed and read. But the internal memory cannot be removed easily or read without somehow powering up the PDA. Furthermore, some PDAs lose data if their internal batteries are not kept charged up. If a PDA is to be regarded as prime evidence, then advice should be sought to ensure that critical data is not lost after seizure and before a case comes to trial.

[31] There may be explicit or implied authorisation under an employee’s contract of employment. In addition, it is possible to seize a computer under a warrant.

Specialist forensic tools have emerged. At the time of writing, Paraben[32] has a collection, although EnCase also offers some facilities. In addition, there are some "free" or Open Source utilities such as *pdd* for Palm[33] and OSImage and Dumpprom for Pocket PCs. There is a useful overview available from the US National Institute of Science and Technology[34]. Precise technical procedures vary between PDA "families". In the Palm family there is a hidden command which puts the Palm into "console" mode, whereas Pocket PCs have to be imaged via the "ActiveSync" program. PDAs use a variety of connectors to link the PDA to a PC so that one of the earliest tasks of the technician is to ensure that they have access to the correct hardware for the job in hand. Because of the many opportunities to make mistakes, technicians are advised to provide fuller than usual contemporaneous notes.

Depending on the circumstances, it may be necessary or appropriate to use a lesser technique for capturing essential information. The large PDA families, Pocket PC and Palm[35], have achieved their popularity in part from the ease with which information can be shared between the portable device and a PC, capturing the PC files (Palm terms this "Hotsyncing" and PocketPC terms it "ActiveSync"). However, not all information on the PDA is copied to the PC. The safest route is to secure the PDA and await proper imaging by trained personnel. Detailed technical advice has been produced by US National Institute of Standards and Technology[36].

### *Legal Issues*

These are similar to those regarding PCs. In admissibility terms the entire PDA is "real evidence". However, there are significant hurdles in terms of getting full legal access to a PDA where the owner does not want to cooperate and the PDA is personal property, not that of the business. Unauthorised access may be a criminal offence and there may be data protection and human rights issues.

## *Cellphones*

The first cellphone, as opposed to a radio or walkie-talkie which could be linked to the telephone network, dates from 1973. Modern cellphones, as available in 2008, provide much more than the ability to provide on-the-go communications to any telephone, fixed and mobile, anywhere in the world. They often have substantial PDA functionality – contact lists, diaries, stored files, photographs, etc and may also feature in-built cameras. As with PDAs they can synchronise with personal computers.

[32] http://www.paraben-forensics.com/catalog/index.php?cPath=25&osCsid=4a67143f86e68754330bc45c3eea12e3

[33] Http://www.grandideastudio.com/portfolio/index.php?id=1&prod=17

[34] http://csrc.nist.gov/publications/nistir/nistir-7250.pdf

[35] Some PDAs also use a version of the Linux operating system.

[36] *Guidelines on PDA Forensics*, available at: http://www.iwar.org.uk/comsec/resources/nist/pda-forensics-sp800-72.pdf

In addition to making conventional telephone calls, many cellphones can also make data calls and link to the Internet both to browse the world wide web and to provide mobile email. Increasingly almost any Internet service which is available to desk-top and laptop computers is also available on a cellphone. Connectivity may not end there; some cellphones have wi-fi facilities and connect wirelessly to local area network. The use of Bluetooth connectivity is also wide-spread; Bluetooth can be used, among other things, for wireless headsets, to connect a cellphone to a PC, to connect to other cellphones, and also to some sat-nav systems.

It is the complexity and variety of cellphones which provide the corporate investigator with many potential headaches – plus the fact that new models appear all the time. Unlike PCs, where most corporate machines will use the Windows family of operating systems or Mac OSX, each cellphone manufacturer may develop their own operating system. There are some broad families of cellphone operating systems for more sophisticated products – Symbian, Windows Mobile, Blackberry/RIM, Palm, Linux, and "Google" – each of these exists in several variants and there are many instances of customisation to give individual phones their unique specification. It requires a not insubstantial investment by specialist investigators to maintain a collection of connectors, cables and software for the range of models they are likely to be asked to examine.

There are two big problems as well as some more minor ones facing anyone seeking to preserve a cellphone for evidential purposes: how to ensure that existing data on the phone does not become over-written or otherwise lost, and how to extract all the data that might be there.

A cellphone seized in a power-on mode is by definition ready to receive calls and SMS messages. When voice and SMS messages are received, the registers in the phone which log such matters are updated. But a cellphone once switched off may be protected with a PIN and not be capable of being restarted without the co-operation of the owner. Some cellphones, though fewer than in the past, have volatile memory which means that if a battery is allowed to run down, some of the data artefacts will be lost. One solution to the "let's keep the phone on to preserve memory but stop it from receiving calls" problem is to place the phone, switched on, but within a Faraday cage, in effect a grounded metal box or metallic bag. But when you do so, the battery will then almost certainly exhaust itself more rapidly, as the phone may think that it is simply out of range of a base station and will increase transmission power.

Turning now to the basic function of making and receiving telephone calls: each phone gets its identity in two ways: the SIM or Subscriber Identity Module[37] is what identifies the caller to the phone network and also provides the means of payment, which will be either on a monthly contract or be topped up on a "pay as you go" basis. The IMEI or International Mobile Equipment Identity is what uniquely identifies any particular item of hardware. Cellphones have two, sometimes, three areas where unique, investigation-relevant, information may be held. The SIM in addition to holding immediate information about the phone's number, its IMSI and its location area identity, will also hold contact details and SMS messages. The body of the phone also has an area of "addressable" data storage and this can include, contact

[37] USIMs are the equivalent for UMTS or 3G services

details, SMS messages and will also contain details of recent phone calls made, received and missed. Finally many cellphones also have slots for external storage cards such secure digital, micro-digital etc.

What this means is that if it is considered appropriate or helpful to seize a mobile phone as potential evidence it is essential to have proper professional assistance available at a very early stage.

Because of the volatility issues mentioned above it is especially important that proper time-stamped contemporaneous notes are kept. For example:

- Was the phone switched on at the point it was acquired?
- Were any arrangements made to keep the battery charged?
- Is there a photograph of it (especially its display) at the time of seizure?
- If it was switched on, what decision was made about leaving it powered on or switching it off, and why?
- Were any phone calls or messages received before it could be passed to a technician?
- Were any inspections of call registers, etc made because of perceived operational necessity? Are all of these fully documented?

The Netherlands Forensic Institute has produced two useful documents:

- A "principles" document which shows how the ACPO principles for handling computer evidence in general can be applied to mobile phones: http://www.holmes.nl/MPF/Principles.doc
- A work-flow document which shows the steps required in a proper investigations of a mobile phone: http://www.holmes.nl/MPF/FlowChartForensicMobilePhoneExamination.htm

Another source of guidance comes from the US National Institute of Standards (NIST) for the Department of Homeland Security:
http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

There are only two areas of technical investigation which are open to those without specialist equipment and training and both of these are quite limited.

- Many cellphones come with software to "sync" (synchronise) or provide back-up to a PC. The actual facilities within the software can vary quite considerably: some back up key settings, some provide synchronisation with well-known PC applications such as Microsoft Outlook and share with it contact details, diaries, notes and "tasks". Provided that access to the computer is available and it has been properly imaged and preserved it is worth looking for the presence of cellphone "syncing" software such as Microsoft Active Sync, Palm HotSync or Nokia PC Suite to see what data is associated with them. Almost certainly if they are present and configured they will be linked to the Outlook, Outlook Express or similar.

- The SIM can be removed and some of the contents can be read in the very low-cost reader devices sold to allow regular users to back them up or transfer phonebook and live SMS details from one cellphone to another. But these devices are usually not capable of reading all the data on a SIM card or of recovering deleted data.

The URL: http://www.e-evidence.info/cellarticles.html is a good source of further reading and an indication of the availability and capabilities of the facilities on offer to specialist technicians.

### *Legal Issues*

These are similar to those regarding PCs and PDAs, though with the additional difficulty that telephones might be regarded as more "personal" than other devices thus setting the bar on the tests of necessity and proportionality that bit higher. In addition, voice and SMS messages which are intended for the owner of the phone have been intercepted and have not been received by the intended recipient may fall foul of the Regulation of Investigatory Powers Act 2000.

In admissibility terms the entire cellphone is "real evidence". However, there are significant hurdles in terms of getting full legal access to a cellphone where the owner does not want to cooperate and the PDA is personal property, not that of the business. Unauthorised access may be a criminal offence and there may be data protection and human rights issues. It might be prudent for an organisation that supplies cellphones to its employees to address the issue of employee rights to privacy explicitly in the contract of employment or similar document.

### *Cellsite analysis*

An investigatory route available to law enforcement is cellsite analysis: the ability to track the movements of the owner of a cellphone using signals detected from that phone whether or not a call is in progress. The global cellphone system relies on the existence of a large number of local base stations which link the cellphone to the rest of the telecommunications network. Each cellphone provider has to know at any one time the location each of its customers – those with their phones switched on – so that a call can be initiated through the closest base station. In order to make this possible, powered-up cellphones are constantly exchanging brief messages with nearby cellsites and "registering" with them. This registration data is retained by the cellphone company and can be supplied, against the appropriate warrant, to law enforcement. By correlating the signal data over time and by triangulating against the location of the base station masts, a reasonably accurate picture of the movements of a cellphone owner can be built up. The level of accuracy depends on a number of factors, including the density of base stations in the relevant vicinity, the absence of data misreadings, the result of signal bounce and distortion which can result from high buildings and other terrain features, and the level of traffic on the base stations.[38]

[38] If a base station is "full" of active connections it may offload traffic to another nearby base station.

The main limitation on this technique in private as opposed to law enforcement investigations is that the cell site location data is unlikely to be released other than against a proper law enforcement-sponsored warrant.

There is one exception, where the owner of the cellphone has consented to be tracked. Such services are available in a number of countries, including the UK. Typical customers are parents anxious about their children and businesses needing to identify the location of some of their employees. The UK services require customers to go to significant lengths to demonstrate that consent has been obtained.[39] Versions of Google maps for running on some mobile phones use the same technique in order to deliver a "show me where I am" service. GPS-based services are much more accurate for these location-finding facilities.

## *Other Storage Media: Cameras, Thumbdrives, Media Players and Other Portable Media*

The physical size of media in relation to the amount of data held continues to plummet, as does the variety of devices upon which they can be found. Digital camera media, Compact Flash, Secure Digital, etc. can hold any kind of data, not just photographs. USB "thumbdrives" with a capacity of 2Gb cost under £100 in late 2005 and about £30 one year later in 2006. A year later still, and the cost had fallen well below £10. In 2000 most laptop computers had hard disks with less capacity. 2Gb is also equivalent to three fully-filled CDRoms. Memory cards as used in camera and media players are smaller than a postage stamp – 8 GB can be bought for under £20. Many portable disk drives and music players, with typical capacities of up to 1000 GB (1TB) and priced as low as £50, are capable of being secreted in a modest-sized pocket. Only the most careful examination of a computer will reveal whether any of these devices have ever been connected to it[40]. Yet a company's entire financial records, list of customers, research and development programme can be secreted easily even within a device of 2Gb capacity. The same goes for 100,000 web-sized photographic images.

Most of these classes of media operate in a similar fashion to hard disks in that often deleted data can be recovered. So it is important that any devices suspected of holding data relevant to an incident or investigation are seized and properly imaged.

### *Legal Issues*

The main legal issue in a corporate, non-law enforcement inquiry is that the devices may be the personal property of a suspect and there may be no immediate and timely basis upon which they can be seized.

[39] An example can be seen at: http://www.followus.co.uk/mobilephonelocationandyou.htm
[40] You would need to examine the System Registry

## *SatNav Devices*

Early satellite navigation devices featured maps of limited detail, were relatively difficult to input data to, and were too expensive for most sections of the public. But during 2006 in particular prices fell dramatically and the specifications of models available increased. So ubiquitous have they become that in 2007 the UK Office of National Statistics included satnav devices in the basket of 650 goods and services which it uses to measure inflation.

With increasing sophistication has come greater possibility of useful forensic examination. More expensive satnav devices contain hard-disks, lower end models use memory cards.

For the forensic examiner the problems are similar to those for PDAs and cellphones. There are few common standards other than NMEA, which is the protocol by which data is transmitted by the satellite and available to be interpreted electronically. Each manufacturer has its own ideas about the internal design of their satnav units, and these develop and change with the appearance of new models. The popular TomTom family of devices appears to use a variant of Linux. Some manufacturers rely on a modified form of Windows Mobile.

Typically what is stored includes: recent destinations, saved home and destination addresses, uploaded “Points of Interest”. Most units sold for use in cars do not retain data about specific journeys Navman devices seem to hold some records and sometimes it is possible to recover deleted material from some TomTom devices. Hand-held devices as sold to trekkers, on the other hand, often have a “breadcrumb” facility which records the journey (and which is useful for those who get lost and wish to return to their starting point or plot their journeys afterwards on a terrain map).

Some of the more sophisticated devices can be linked to PCs for back-up purposes, to receive updates and to plan journeys – the software for TomTom devices is called TomTom Home. As with syncing software used for PDAs and Cellphones it is often a good idea to see if there is a computer with whom syncing has taken place and if any useful information exists on it.

### *Legal Issues*

The main legal issue in a corporate, non-law enforcement inquiry is that if the device is the personal property of a suspect there may be no immediate and timely basis upon which they can be seized. Even if the device is provided by the employer, the right to seize may be limited unless there has been some warning in the contract of employment.

In making a decision to seize, an investigator has to consider what contribution the satnav might have to the overall aims of the investigation. If there is a general concern that a vehicle might be misused (or stolen) an embedded satnav device with a link to a mobile phone which can collect data from it at will may be a better choice.

## *Telecommunications data and content*

There are a modest number of practical problems in gathering telecommunications data and content from corporate sources, but these are dwarfed by the legal hurdles.

### *Analogue Telephony*

This covers conventional telephone calls taking place on or through corporate switchboards (PABXs).  Such switchboards routinely provide data about the numbers called and the time and duration of calls.  They do so in order to monitor costs for external calls and to check on service quality in respect of internal calls.  The logs produced can be of considerable value in many kinds of investigations.  To capture the contents of such calls a recording device – tape or disk – is placed across the relevant lines.  Some businesses routinely record phone calls as a check against disputed transactions, or to see whether their employees are misbehaving.

In a forensic situation, the immediate and important issue is to be able to demonstrate that the logs and/or recordings are reliable and have not been tampered with. For the logs:

- it is helpful to be able to say something about the specific PABX and what logging facilities exist;
- there should be some statement about how they were collected, by whom, what precautions were taken, and how selections of data were made;
- once taken, they should be subjected to some form of integrity check, such as MD5 digital fingerprinting, as a guard against post-capture tampering.

For voice monitoring:

- it is helpful to be able to say something about the specific facilities used;
- there should be a statement about what precautions against partial capture were taken and how selections of conversations were made in terms of counterparties, periods of time and so on;
- once taken, the logs should be subjected to some form of integrity check, as a guard against post-capture editing.

The real difficulty is establishing a legal basis on which to carry out the monitoring of internal telephone communications data and content (this is reviewed below and in Appendix 4).

Companies and private individuals can request from their telephone companies copies of their own past telephone bills and detailed call records. Since this is their own personal data there is no conflict with data protection legislation. In practical terms, and because telephone companies must comply with a telecommunications directive (Directive 97/66/EC of the European Parliament) not to hold personal data longer than is necessary for business purposes, call records for earlier periods may not be available.[41] Most telecommunications companies will make a charge to supply historic information.

### *Data Traffic*

There is little practical difficulty for an organisation to monitor data traffic on its own internal networks. In effect, one or more network cards are set up in areas of high traffic flow and instead of just listening for packets of data specifically directed at the associated workstation, all the passing data is collected (putting the card into "promiscuous" mode) and then filtered according to various criteria. Such facilities are used regularly to monitor the quality and load of data traffic on a network and to carry out a variety of technical diagnostics. In the situation of an investigation it is trivial to switch such facilities to monitoring activity by workstation, user identity, email name or the occurrence of specific words. Forensically, the technical issues to be covered in a witness statement include the following:

- can the organisation provide a brief technical description of the monitored network?
- can the organisation identify and describe the technical facilities, hardware and software used to carry out monitoring, including the location of the monitoring points on the network?
- can the organisation describe and provide the raw logs that were generated during the monitoring, and say how it preserved them?
- can the organisation describe any post-capture processing that was carried out to analyse the logs and produce more understandable derived exhibits?

In certain circumstances some organisations may be unwilling to be wholly candid in revealing all about their internal networks. In that event, careful calculations need to be made of the balance of advantage in refusing disclosure requests (with the possible result that crucial evidence is disallowed) and the chances that litigation or prosecution may fail.

#### *Legal Issues*

As with the surveillance of internal telephone calls, the real difficulty is establishing a legal basis on which to carry out the monitoring of data activity (this is reviewed below and in Appendix 4).

[41] This Directive has been modified by Directive 2006/24/EC which is implemented in the UK as the Data Retention (EC Directive) Regulations 2007. http://www.opsi.gov.uk/si/si2007/uksi_20072199_en_1. At the time of writing there is a Data Communications Bill before Parliament. The effect is likely to be extend the period during which data is retained.

Subject to obtaining appropriate authorities and warrants, law enforcement and other government agencies have access to material from public telecommunications businesses which include land-based telecom companies, mobile phone companies and ISPs.

The main law is the Regulation of Investigatory Powers Act 2000 (RIPA 2000). Briefly, this makes it unlawful to intercept any communication in the course of transmission without the consent of one of the parties or without lawful authority. English law is unusual in that it makes a distinction between interception of communications or traffic data (who called who, when and for how long) and content (what was said). Traffic data also includes location data such as where a mobile phone company holds records on which specific base station a given mobile was registered at any one time. Some data held by ISPs or collectable by them is also classified as "communications data". Warrants for interception of content can be issued only by the Home Secretary and are subject to various criteria, which include "the interests of national security", "for the purpose of preventing or detecting serious crime" and "for the purpose of safeguarding the economic well-being of the United Kingdom". The Home Secretary has to be convinced that such interception of content is necessary in relation to other possible means of obtaining the same information and proportionate to the circumstances. Section 17 excludes content evidence from most legal proceedings and also forbids any disclosure that interception of content has taken place.[42] Chapter II of RIPA 2000 (ss. 21–25) covers the circumstances in which authorisations and notices to collect and disclose communications data are issued and by whom. The grounds on which such authorisations and notices may be issued include the following:

- "in the interests of national security";
- "for the purpose of preventing or detecting crime or of preventing disorder";
- "in the interests of the economic well-being of the United Kingdom";
- "in the interests of public safety";
- "for the purpose of protecting public health";
- "for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department";
- "for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health"; and
- for any other purpose specified by an order made by the Secretary of State.
-

There is a lengthy and complex list of "designated persons" who can issue authorisations, but such authorisations have to be necessary and proportionate to the circumstances. There are arrangements to make payments to meet the cost of the telecoms companies, etc.

[42] At the beginning of 2008 the Government announced that it might consider changing the admissibility rules about the content of traffic, but only in respect of terrorism offences and serious crime and subject to a number of limitations. At the time of going to press a report has been published - http://www.official-documents.gov.uk/document/cm73/7324/7324.asp - but the matter is still being reviewed.

Communications data is admissible in evidence. It may be used not only to show that a conversation took place at a particular time but also to show patterns of contact which may in turn suggest relationships between those involved.

The scope for a private company to get access to records from a public telecommunications service without the assistance of law enforcement or one of the other agencies empowered under Part II of RIPA 2000 seems extremely limited.

The debate continues as to whether the UK is wise to maintain the distinctions between content and communications data. Most of the public debate is about the relative risks of losing important cases because content cannot be produced and the possible issues of disclosure of precise methods. But once one leaves the world of conventional telephones, where there is a clear technical distinction between content and communications (tariff and connection data versus recording voices), within most forms of data communication such as email, web-browsing and Voice over Internet Protocol (VoIP) telephony, the clear technical distinction no longer exists and the courts may have to interpret the legislation. They may only be able to do so by examining material that may turn out to be "content" and therefore both inadmissible and which should be excluded from legal proceedings.

## *Data from Internet Service Providers*

ISPs provide what is in fact a bundle of services to customers. Typically, these include:

- connection to the Internet;
- facilities for emails to be sent from the customer to others on the Internet;
- facilities for emails addressed to customers to be received by the ISP and then held until such time as the customer requests the emails, either by connecting or opening their email client;
- facilities for hosting websites so that they are permanently available to the world wide web. These websites may be simply "static" – that is, containing information that does not change very frequently, or may be full-scale e-commerce sites capable of taking orders from the public, linking to credit card authorisation schemes, confirming details of sales and originating computer records for the vendor to translate into despatch of orders;
- facilities such as newsgroup feeds, hosting for chatrooms, etc.

In legal terms an ISP is for some of these functions a "common carrier", in the same way as a conventional telecoms company specialising in voice telephony. But for other functions such as hosting websites, the ISP is more like a publisher.

The operation of a ISP generates various logs which are essential to its business, either in terms of maintaining quality of service or for tariffing. From the perspective of law enforcement the most important of these is the Remote Authentication Dial In User Service (RADIUS) log. In order to communicate on the Internet each user needs an IP (Internet Protocol) address, which has the form 123.123.123.123 (four triplets separated by dots). There are currently insufficient numbers of these to provide unique permanent IP addresses for everyone who communicates on the Internet, so in practice each ISP has a pool of addresses which it assigns on a temporary basis to its customers. Thus, if an organisation is interested in the identity of someone who is communicating with it and their IP address is obtained (a relatively simple technical procedure), it will need to discover (from Internet resources) which ISP owns that address. But it will only be by reference to the RADIUS log that the actual identity of the person can be revealed.

*Legal Issues*

If ISPs operate in the UK, they can readily provide customers with their own personal data that the ISP holds about them. But for most purposes, ISPs cannot supply data on third parties other than against a proper authorisation under RIPA 2000 or an explicit court order. Again, in relation to a website that an organisation may have had hosted by an ISP, the ISP can provide the organisation with such web logs as it has collected and the organisation is prepared to pay for. But logs from the websites of third parties are unlikely to be available in the absence of authorisation under RIPA 2000.

Emails held on the ISP's mail server computers will be regarded almost certainly as being on a public telecommunications service for the purposes of RIPA 2000. To obtain traffic data, law enforcement will require an appropriate authorisation under Chapter II of RIPA 2000 but that evidence will be admissible. To get the content a warrant signed by the Home Secretary will be necessary, and the material can only be used for intelligence purposes but will not be admissible as evidence.

## *Evidence from the Web*

An organisation may have come across something on a remote website and thinks that it may be needed for evidence. It could be an offer of something for sale after a transaction has been completed or it could be defamatory. How does an organisation capture it?

One route is simply to use the "Print" option within the browser. Most browsers will not only print out what you can see on the screen but also provide a footer with details of the URL (website and specific page) together with a day and time stamp. As with other printouts, the result is better than nothing but also open to the charge of ease of subsequent alteration. The same could be said of "saves" to disk. Both Microsoft Internet Explorer and Mozilla Firefox gives options to save "Web Page Complete" and "Web Page HTML only", but here too, post-capture modification of content is easy.

There are programs that can capture an entire website or part thereof. One example is Webwhacker[43], which can preserve the directory structure of a website and save it to external storage such as a CDRom for later examination. The process is sometimes called "spidering". In addition, the program can monitor a website for changes, which may be useful during an investigation.

There are some important limitations that need to be considered. The first is that what can be seen on screen is not necessarily what is currently on a remote site due to the caches kept by ISPs and on Internet browsers. A further complication is that what is being seen on screen may have been assembled from a number of sources and in quite complex ways, as when the web designer has used "frames" or "cascading style sheets". Older web-capturing tools may fail to "get" every single element.

All this means that both web-capturing and writing accompanying witness statements have to be carried out with some care in order to anticipate criticism.

The second limitation is that spidering only works when the webpages have fixed content: that is, they exist as files on the remote website. But on many websites the pages being seen are created "on-the-fly" against a specific request or in response to specific circumstances – this is known as dynamic page creation. Examples include the "results" pages created by search engines such as Google, the "welcome" page on Amazon.com where, in response to a cookie on your computer, you are greeted by name and with a list of uniquely personalised "recommendations" based on previous purchases, as well as the accumulated shopping baskets that almost all e-commerce pages have.

In these circumstances the only evidence an organisation may be able to collect is a "controlled" printout: one where careful contemporaneous notes are written up during the process, in the hope that this will be sufficient to persuade a court. Web travels may leave information in the cache which, when reviewed in a cache analysing program such as Netanalysis[44], may provide corroboration – however, not all e-commerce pages are captured in the cache[45]. Ways around this include the use of a video camera to record onscreen activity, or programs such as Camtasia, which sit in the background and save snapshots of the screen to a movie file – the program is used to develop computer training modules.

## *Evidence from Web Servers*

This is the other side of the same problem. An organisation may own a website and wish to assert that it has been publishing certain items of information, or it may wish to demonstrate that certain individuals have been visiting the site at particular times and carrying out certain types of activity.

[43] Http://www.bluesquirrel.com/products/webwhacker/. Other examples include Pagesucker: http://www.pagesucker.com/ and Surfsaver: http://www.surfsaver.com/

[44] Http://www.digital-detective.co.uk/intro.asp.

[45] To prevent double-ordering, or the subsequent retrieval of sensitive financial information.

Web server programs, among which the most popular are Apache and Microsoft Internet Information Services, can be set up easily to collect activities into a log. These logs are usually in Common Log Format (CLF), although it is possible to collect additional information. From a forensic perspective, these logs are no different from other types of computer log that one may wish to offer in evidence.

In terms of the overall reliability of web server logs, the following elements in a witness statement may help to persuade a sceptical court:

- a description of the computer system's overall functions and the role of the web server within it;
- an account of how long the system in its present configuration has been in operation;
- what forms of testing took place prior to commissioning and what forms of routine audit are in place;
- what external factors exist to act as a check on reliability;
- what security features exist and how they are managed (this is anticipates suggestion that incriminating material was placed there by someone other than the suspect);
- whether other similar systems are in existence that have a good history of reliability;
- compliance with any external good practice or system audit standards.

In terms of the precise exhibit that is being produced, it is useful to be able to say:

- how the selection of the data in the exhibit was made and why it can be regarded as "complete" in terms of the issues at hand;
- what procedures were used to collect the evidence such that it can be regarded as free from tampering;
- what procedures were used to preserve the evidence so that it can be regarded as free from subsequent tampering – this may take the form of imaging some computers or copying selected files to write-once data media such as CD or DVD, or making a digital fingerprint of the files;
- what manipulation or subsequent analysis was carried out to make the material "easier to understand" – this is a perfectly legitimate course of action, but in this event the original material should be exhibited so that the defence team can test the manipulation or analysis.

Usually, admissibility of evidence will be on the basis that the material is a "business record" as defined in is a "business record" as defined in s. 117 of the Criminal Justice Act 2003.

## *Evidence from Computer Intrusions*

An interesting issue arises when an investigator wishes to make a covert entry into a suspect's computer across a network or the Internet. At a technical level, this is a relatively easy task: any of a number of Trojan horse and remote administrator programs will accomplish this. Facilities for capturing each keystroke on a computer or collecting screen snapshots at regular intervals (keylogger programs) are also widely available and usually operate covertly.

However, for the corporate investigator there are significant legal hazards. Any such entry without authorisation from the computer owner is an offence under the Computer Misuse Act 1990. Even if the computer is owned by the investigator's employer, the computer user has a reasonable expectation of privacy and the circumstances must be such that these expectations can be overcome – for example, because of a term in the employee's contract of employment (see Appendix 4 for the general problems of employer surveillance of employees).

For law enforcement it is possible to get a warrant for intrusive surveillance under s. 26(3) of RIPA 2000. (edit note: problems with these two lines)
Section 32(3) sets out the circumstances in which such surveillance has to be justified, and there are overarching tests of necessity and proportionality[46]. There are a number of problems for law enforcement: it may wish to avoid disclosing its precise methods and, although it is possible for law enforcement to approach a judge under the public interest immunity agenda, this may be at the expense of not being able to use the result of the intrusion.

In addition, there is a "reliability of evidence" problem: how can the investigator reassure the court that the evidence on the computer submitted has not been tampered with? Essentially, once the investigator is inside the computer, all assurance of the integrity of any evidence derived vanishes – it is no longer possible to state categorically that the evidence has not been tampered with. At worst, if in a criminal case defence lawyers suspect that their client has suffered a law enforcement intrusion, even if no evidence has been adduced by the prosecution, they may have powerful arguments for claiming that the evidence is so tainted that the trial should be abandoned.

## *CCTV equipment*

Early forms of closed circuit television consisted of a low-cost, low resolution camera linked by coaxial cable to a monitor; if it was desired to record activity, it was to a tape-based machine, usually one which ran much more slowly than a conventional VCR so that the tapes did not have too be changed too often. The use of hard-disk-based recording has had many advantages: it is less prone to wear than tape, hard-disk capacities permit long periods of usage, indeed a recorder can be set to re-use hard-disk space automatically after, say, seven days of usage; time-codes are much easier to enable – this is crucial if you want to examine activity at particular known points; there are a wide variety of compression levels available depending on the desired quality of the recorded video; multiplexing of several different cameras can take place on just the one recording medium. More modern cameras can also use network protocols and cables instead of coaxial cable; indeed they can use wireless networking which greatly eases and reduces the cost of installation. Finally for more advanced systems, once the video is in digital form, software can be used to analyse recorded activity.

[46] A code of practice can be found at: http://www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codeofpractice/surveillance/part1.html

It is the digital element in modern cctv that justifies its inclusion in this section of the guide. The problem is that there are few established standards for recording cctv video on to hard-disk. Most of the systems are proprietary to their individual manufacturers and it can be difficult to extract video streams of even still pictures therefrom without the aid of the manufacturer. The hard-disks inside cctv recorders can nearly always be removed and subjected to forensic imaging. But thereafter without the specific software in the cctv recorder (often firmware, software installed on a microchip) the disk operating system and the precise method by which the video was recorded to disk, the forensic disk analyst may not be able to view the video.

Indeed one of the major problems faced by law enforcement is that, in a complex enquiry, in order to follow the activities of people of interest, they require to look at the recorded output of large numbers of different systems, all in different formats.

A Home Office publication, http://www.crimereduction.homeoffice.gov.uk/cctv/cctv36.htm gives some useful assistance to those contemplating a new or revised cctv system. Much of it applies to organisations that think the main use of their cctv systems will be in internal investigations, as opposed to providing assistance to law enforcement. The following is a summary:

In order to ensure the evidential value of pictures, your CCTV system should meet the following requirements:

**Quality - Are the pictures good enough?**

- Before installing a CCTV system you should have a clear idea of what you want the system to do and how it should perform (e.g. recognise the face of someone walking through a doorway, or read a vehicle registration number).
- It should not be expected that enhancement features, such as zoom controls, would provide extra detail. If you can't see it, then it's not fit for purpose.
- You should test the system using a volunteer etc.
- The quality of the recorded or printed pictures may differ from the live display.
- Ensure the time and date on the system are correct.
- The quality of the pictures should not be compromised to allow more to be squeezed onto the system.
- Regularly maintain all aspects of the system (e.g. camera focus, cleaning of lenses, etc).

**Storage - Are the pictures stored appropriately?**

- Access to the system and recorded images should be controlled to prevent tampering or unauthorised viewing.
- A record should be kept of who has accessed the system and when. Further information on this can be found in the BSI document 'Code of Practice for Legal Admissibility of Information Stored Electronically' (BIP0008) or from your local Crime Prevention Officer.

- Physical protection methods such as locked rooms are just as effective as electronic protection methods that require proprietary software or hardware. These can hinder the police's investigation.
- It is important that recordings are retained beyond 31 days if possible.
- It should be possible to protect specific pictures or sequences, identified as relevant to an investigation, to prevent overwriting before an investigator can view or extract them.

### Export - Can the pictures be easily exported from the system?

- A trained operator and simple user guide should be available to assist the investigator in replay and export.
- Export of medium and large volumes of data can take a substantial period of time. The operator should know the retention period of the system and approximate times to export different amount data.
- If the software needed to replay the pictures is not included at export, the police may have trouble viewing it. Export of a system event log or audit trail, and any system settings with the pictures will help establish the integrity of the pictures and system.
- The system needs to be capable of exporting small or large amounts of video quickly without losing quality. An ideal solution for medium-to-large downloads, would be for the system to have the facility to export to a 'plug-and-play' hard drive.
- The system should not apply any compression to the picture when it is exported as this can reduce the usefulness of the content.

### Playback - Can the pictures be easily viewed by authorities?

- The replay software must allow the investigator to search the pictures effectively and see all the information contained in the picture and associated with it.
- It should be possible to replay exported files immediately, e.g. no re-indexing of files or verification checks.

Further information can be found at:
http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/

*Legal Issues*

The use of CCTV on employees falls squarely within the guidance given in Appendix 4 of this guide, which addresses the broad issues of employers' rights to carry out surveillance on their employees.

If the CCTV is aimed at non-employees including members of the public, the main laws to worry about are Human Rights and Data Protection. The essence is that an organisation has to be clear what the reasons are for the installation and to make sure that the way the system is set-up does not cause any intrusion beyond that necessary and proportionate to achieve those goals. Typical aims would be theft reduction and public safety. But the privacy of individuals must still be respected. For example cameras should not be pointed at areas where people have a reasonable expectation of privacy and where there are no specific grounds for believing that wrong-doing can be spotted there, as opposed to other locations. More intrusive surveillance of identified individuals would also need to pass the necessity and proportionality tests: for example that they had appeared to carry out activities consistent with theft.

In relation to the storage of cctv recordings in which people appear (including those recordings in digital form), the standards used must be meet the eight data protection principles as the video recordings will count as "personal data": the data must be

- fairly and lawfully processed.
- processed for limited purposes and not in any manner incompatible with those purposes.
- adequate, relevant and not excessive;
- accurate.
- not kept for longer than is necessary.
- processed in accordance with individuals' rights.
- secure.
- not transferred to countries without adequate protection.

The Information Commissioner has issued a Code of Practice: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

# Appendix 3: Admissibility of Evidence from Computers

The word “admissibility” refers to legal rules that are applied to an item of potential evidence before a court can consider the value of the facts that it purports to offer. This Appendix provides an overview of the issues.

If a device is simply recording information as in, for example, automated records of telephone calls, or who entered a building at a particular time, or an amount of fuel dispensed, evidence from such devices is admissible as “real evidence”. To qualify: there must no possibility that the recording can be adjusted or manipulated – it must be a “dumb”, automated process.

If an entire computer or some item of data storage media (disks, tapes, etc.) are seized and can be offered in court, they are admissible as “real evidence”. Anything derived from this real evidence – printout, display, CDROM extracts, the product of analysis – becomes a separate exhibit, admissible when the person who carried out the derivation is present in court and can formally produce the exhibit and be cross-examined.

Up until April 2000 there was a separate admissibility regime for computer evidence which required a certificate that the computer was operating properly and was not used improperly, before any statement in a document produced by the computer could be admitted in evidence (the former s. 69 of the Police and Criminal Evidence Act 1984). But today a presumption exists that the computer producing the evidential record was working properly at the material time and that the record is therefore admissible as real evidence. However, this presumption can be rebutted if evidence casting doubt on its intrinsic reliability is adduced.. In this event it will be for the party seeking to produce the computer record in evidence to satisfy the court that the computer was working properly at the material time.

Nevertheless, documents found on a computer may be “documentary hearsay” – although the existence of the document on a computer is admissible, its contents may need to be separately admitted.

A printout or substantive computer file is a document if:

- the document was created or received by a person in the course of a trade, business, profession or other occupation, or as the holder of a paid or unpaid office; and
- the information contained in the document was supplied by a person (whether or not the maker of the statement) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with.

It then becomes admissible as “business document” for the purposes of s. 117 of the Criminal Justice Act 2003. The court may make a direction if satisfied that the statement's reliability as evidence for the purpose for which it is tendered is doubtful in view of-

(a) its contents,
(b) the source of the information contained in it,

(c) the way in which or the circumstances in which the information was supplied or received, or

(d) the way in which or the circumstances in which the document concerned was created or received.[47]

Communications data acquired under warrant is admissible and normally will be produced by a telecoms company or similar using the business records rule under s. 117 of the Criminal Justice Act 2003. As we have seen, currently content is not admissible under s. 17 of the Regulation of Investigatory Powers Act 2000 (RIPA 2000). However, content is admissible if it has been obtained from an overseas law enforcement agency within its own jurisdiction and is subject to the availability of someone to produce it before the English court.

Expert evidence has been admissible in English law since 1782 and there are cases going back to 1554. But "expert" for this purpose means the right of the witness to offer opinions based on experience. This is distinct from the role of a forensic technician who may have carried out a technical investigation or procedure and simply reports factually on their findings. In the end it is for a judge to form a view of the extent of any individual's "expertise" and hence the territory over which opinions can be offered.

Traditionally English law excluded so-called "bad character" evidence – that is material which is not directly linked to the suspect events but which might show that an accused has a propensity or proclivity towards certain types of activity. Until 2003, defence lawyers were able to ague that such material was "prejudicial". But the Criminal Justice Act, 2003, introduced a number of circumstances in which a judge, after applying some tests, could allow the evidence to go before a jury. The details appear in Part II Chapter 1 of the Act – sections 98-113. Increasingly investigators are examining computers of suspects in the hope of finding, if not direct evidence of wrong-doing, but material which meets the tests laid down in the Act. These tests include "important explanatory evidence", "matter in issue between the defendant and the prosecution" and "evidence to correct a false impression." On this basis indications of websites visited and/or bookmarked as a favorite or some email traffic may now be adduced in evidence.

A judge has general discretion to exclude any evidence which appears to be so unfair (normally by reference to the way in which it was obtained) that it would have an adverse effect on the fairness of the proceedings; s. 78 of the Police and Criminal Evidence Act 1984). Normally, judges only make such exclusions on the application of defence lawyers.

Admissibility rules in countries on the European mainland tend to be much more relaxed than in the UK. This is often a function of the different criminal justice procedure. The UK procedure is adversarial – the judge acts as the chair over proceedings in which the evidence and arguments are presented by opposing lawyers. The continental procedure is inquisitorial, dominated by an examining magistrate. Admissibility rules in the US follow the English common law model but have evolved differently. For example, warrants to seize evidence have to be drawn up with much

[47] s 177(7)

more precision than in the UK; material seized outside the scope of a warrant, unless "in plain sight" may be rendered inadmissible.[48] One of the more interesting divergences is the way in which novel scientific and technical evidence is handled. In the UK, the jury is simply presented with opposing expert witnesses (who may have been asked to identify points of agreement and disagreement[49]). In the US, novel scientific and technical evidence is an admissibility issue, with the judge acting as a gatekeeper to protect the jury from scientific evidence which has not been established as "generally accepted". Where necessary, a trial before the main trial is held (*a voir dire*) – the *Daubert* rules (see p 27).

[48] More guidance on the US position can be found at:
http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm

[49] Under CPR 33.5: http://www.justice.gov.uk/criminal/procrules_fin/contents/rules/part_33.htm

# Appendix 4: Employer Considerations in Carrying Out Surveillance on Employees

Computer investigations into employees by employers operate under the same constraints and rules as ordinary investigations. Among other things, the individual employee is protected by the following:

- Employment Rights Act 1996;
- Human Rights Act 1998;
- Data Protection Act 1998;
- Sexual Discrimination Act 1975;
- Race Relations Act 1976;
- Police and Criminal Evidence Act 1984.

For example, this last covers the circumstances in which an interview takes place and when a caution should be administered. Two other Acts are particularly important in the IT domain:

- Computer Misuse Act 1990;
- Regulation of Investigatory Powers Act 2000 (RIPA 2000).

Any action by an employer has to pass a test of “necessity” (there was no less intrusive route) and “proportionality” (what was done was limited to what appeared to be strictly proportionate to the circumstances – are you investigating stolen stationery or substantial missing funds?).

In determining a legal policy for any form of surveillance, there are some general principles from which the detail flows:

The basic power in respect of private telecommunication services is found in s 1(6) of RIPA:

> The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if—
>
> (a) he is a person with a right to control the operation or the use of the system; or
>
> (b) he has the express or implied consent of such a person to make the interception.

The detailed rules for legitimate interceptions are mainly to be found in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[50]. To fall within the Regulations, the interception has to be by, or with, the consent of a person carrying on a business, for purposes relevant to that person's business and using that business's own telecommunications system.

Interceptions are authorised for monitoring or recording communications:

- to establish the existence of facts;
- to ascertain compliance with regulatory or self-regulatory practices or procedures;
- to ascertain or demonstrate standards which are (or ought to be) achieved (quality control and training);
- in the interests of national security (in which case, only certain specified public officials may make the interception);
- to prevent or detect crime;
- to investigate or detect unauthorised use of telecommunication systems;
- to secure, or as an inherent part of, effective system operation;
- to determine whether received communications are business or personal communications;
- made to anonymous telephone helplines.

The UK also has a code of guidance for employer–employee relationships. The Information Commissioner's 2005 Employment Practices Data Protection Code[51] states the obligations of employers. It lays down strong principles of data protection, prohibits the making of decisions solely on the basis of automated data, requires employers to notify employees of surveillance policies and places limits on the extent of monitoring which can take place. It requires the explicit consent of employees before sensitive data such as medical or information can be collected. The third part of the Employment Practices Data Protection Code contains a guideline on how firms can legally monitor staff emails. Employers have the right to monitor staff emails, provided that employees have been warned that monitoring is taking place and that the reasons for monitoring have been explained. The Employment Practices Data Protection Code covers a range of surveillance activities including opening emails or voicemail, checking internet usage and recording with closed circuit television (CCTV) cameras, but it also warns businesses that the covert monitoring of employees is unlikely to be permissible unless it is done in response to a request from a law enforcement agency.

[50] The full text of the Regulations is available at : http://www.hmso.gov.uk/si/si2000/20002699.htm

[51] Available at: http://www.informationcommissioner.gov.uk/cms/DocumentUploads/ico_emppraccode.pdf

The Code states that following it will:

- increase trust in the workplace – there will be transparency about information held on individuals, thus helping to create an open atmosphere where workers have trust and confidence in employment practices;
- encourage good housekeeping – organisations should dispose of out-of-date information, freeing up both physical and computerised filing systems and making valuable information easier to find;
- protect organisations from legal action – it will help employers to protect themselves from challenges against their data protection practices;
- encourage workers to treat customers' personal data with respect – it will create a general level of awareness of personal data issues, helping to ensure that information about customers is treated properly;
- help organisations to meet other legal requirements – the Code is intended to be consistent with other legislation such as the Human Rights Act 1998 and RIPA 2000;
- assist global businesses to adopt policies and practices that are consistent with similar legislation in other countries – the Code is produced in the light of EC Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and ought to be in line with data protection law in other European Union (EU) Member States;
- help to prevent the illicit use of information by workers – informing them of the principles of data protection and the consequences of not complying with the Act should discourage them from misusing information held by the organisation.

The Code goes on to give some general principles about monitoring:

- it will usually be intrusive for an organisation to monitor its workers;
- workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment;
- if employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered;
- workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified.

In any event, workers' awareness will influence their expectations.

It says that any organisation that wishes to monitor electronic communications should establish a policy on their use and communicate it to workers. Further detail in the Code suggests specific elements of such a policy. Each specific act of monitoring should be accompanied by a formal impact assessment, carried out by a group of people able to look at all the likely implications.

The Computer Misuse Act 1990 refers to "unauthorised acts" of accessing computers or modifying their contents. In a corporate situation, a business is normally authorised to examine its own computers but the provisions of data protection and human rights legislation still apply. A business is not authorised to access the computers owned privately by its employees – these can include laptop computers, mobile phones, PDAs and data storage devices such as thumbdrives and personal media players,

It is good practice for an employer, or anyone instructed by them to carry out an investigation, to commence with the assumption that they have no powers whatever to investigate – and then explicitly refer to each action in terms of a legal justification. Investigations should always be the subject of contemporaneous notes, which should include actions, decisions and findings.  The role of the investigator's record is to show what was done, when and why.  It provides a response to critics – who may have the benefit of hindsight - and, where relevant, a justification for costs incurred. It should start with the remit of the enquiry and cover every activity within the investigation, including phone calls and informal discussions.

Businesses should also consider creating formal records of decisions which might be construed as impinging on the rights of employees, together with the reasoning behind the decisions.

## Appendix 5: Problems of Disclosure and Confidentiality

For businesses, one of the potentially worrisome features of cooperating with law enforcement in a prosecution or embarking on a civil action is that the "other side" is entitled to disclosure. Indeed, in a criminal matter, someone who is not a direct victim but a third party may find that they are the subject of a disclosure requirement. There is little doubt that on occasion some defence lawyers, lacking any better tactic, have attempted "aggressive disclosure", hoping to thwart a prosecution or civil action by requiring the disclosure of embarrassing or sensitive information to the point where the party concerned decides that it is in their wider interest to withdraw cooperation.

This appendix provides an outline of the law and the issues, but it is stressed that in any individual situation, an organisation will need access to specific legal advice.

### *Criminal Procedure*

The main current law is to be found in the Criminal Procedure and Investigations Act 1996 (CPIA 1996)[52]. There is also a Code of Practice issued under ss. 23 and 26 of the Act. It replaces an earlier and simpler "materiality" or "relevancy" test which was thought to be too vague and liable to abuse[53]. There is also in force a set of guidelines prepared by the attorney-general[54].

CPIA 1996 makes the investigator responsible for ensuring that any information relevant to the investigation is retained, whether gathered in the course of the investigation or generated by the investigation. The investigator is required to draw the prosecutor's attention to anything that might undermine the prosecution case. When evidence is served it must be accompanied by a schedule of "unused material" which the defence team can then ask to see, should it so wish. This is called "primary disclosure".

If material is thought to be "sensitive", it must be listed in a separate schedule. Sensitive material is that which an investigator believes not to be in the public interest to disclose. Examples within digital evidence could include material relating to national security, material given in confidence and material relating to police methods. It is for prosecutors to decide, subject to the law and codes of practice, what to disclose as "unused material" to the defence by way of primary disclosure.

CPIA 1996 imposes on the defence the obligation to produce, in good time before trial, a defence case statement indicating the broad bases upon which a charge is to be challenged. Failure to do so may mean that late-announced defence arguments may be disallowed by the judge at trial. Once the investigator has received the defence case statement, they are under a duty to re-evaluate what has been in the primary disclosure and advise the prosecutor of any further unused evidence which might now undermine the prosecution case. In addition, the defence team can make specific

[52] Http://www.hmso.gov.uk/acts/acts1996/1996025.htm. The Criminal Justice Act 2003 introduces a number of amendments which emphasise the defence's duties as well as the prosecutor's duty of continuing review of matters which might undermine their case and assist the defence.

[53] *R v Keane [1994] 1 W.L.R. 746; (1994) 99 Cr. App. R. 1.*

[54] Http://www.lslo.gov.uk/pdf/guidelines.pdf

requests for disclosure, subject to a materiality test. The prosecutor is under a duty to produce secondary disclosure in reply to a defence statement and is under a continuing duty to review questions of disclosure. If the defence is dissatisfied with the response to a request, or if the prosecutor believes that a request is unjustified by reason of irrelevance to the stated bases of the defence or excessive, resort is made to the court for a ruling.

The precise position of computer-derived materials remains unclear – how much needs to be disclosed? From the investigator's perspective, the quantity of digital evidence that may have been obtained or seized may be so vast that they have not had the opportunity to make an exhaustive assessment of what they have in their possession, and so make a judgment under CPIA 1996 of what ought to be disclosed. The Association of Chief Police Officers' Guidelines currently suggest that the defence should be made aware by way of schedule of this "unused material" and in addition should be warned specifically that neither investigators nor prosecutors have carried out a full review of what might be contained.

There is a further situation to be considered: if an organisation commissions an investigation, the notes for and results of that investigation may also eventually be disclosable to a defendant. The precise circumstances are too complex to explain in detail in this Guide, though some help is available via the *Crown Prosecution Service's Disclosure Manual.*[55] One way to avoid such disclosure is to arrange for any investigator to be instructed not by the organisation direct but by its legal advisors; at that point the results of the investigation are likely to become covered by professional legal privilege.

The basis upon which a prosecutor can withhold disclosure is usually via the mechanism of public interest immunity (PII). This usually takes the form of an application by a prosecutor to a judge. Depending on the circumstances, it is possible for a hearing to be *ex parte* – that is, without notifying the defence. The judge has to weigh the balance between the dangers of disclosure against the need to ensure a fair trial. It is almost never possible for a prosecutor to adduce evidence which has been derived from material which is withheld from disclosure. Public interest immunity simply excludes material which might be relevant to the defence's case.

From the perspective of most commercial organisations, the main heading for allowing "unused" material to be "sensitive", and hence be excluded, is that the material was "given in confidence", but there is nothing automatic about this and a judge may still order to disclose if it is believed necessary.

One route to limit disclosure that sometimes can be pursued fruitfully is to allow a defence expert access to sensitive material, but against a formal written undertaking that the sole purpose of such disclosure is for the immediate legal proceedings. If necessary, a party from whom disclosure is required can ask that the expert's undertakings are covered by a court order. The effect of this is that any unauthorised or *ultra vires* disclosure would be contempt of court.

[55] http://www.cps.gov.uk/legal/section20/chapter_a.html

The victim-owner of a computer may find that law enforcement asks for information under the agency's disclosure obligations. But this may clash with the victim's existing confidentiality obligations. Such matters are normally resolved by a hearing in front of a judge; ultimately the judge can issue an order requiring disclosure but will usually expect to be convinced that such disclosure will result in the production of evidence relevant to the case in hand. Further detail can be found in the CPS Disclosure Manual,[56] but if such an event arises, good specific legal advice is essential.

Procedures for cases of complex fraud may vary from this general explanation.

### *Civil Procedure*

The general rules for the disclosure of "documents" in the English Civil Procedure are to be found in Civil Procedure Rule 31. What is required to be disclosed is set out in Civil Procedure Rule 31.6, which provides:

> Standard disclosure requires a party to disclose only –
> (a) the documents on which he relies; and
>
> (b) the documents which –
> (i) adversely affect his own case;
>
> (ii) adversely affect another party's case; or
>
> (iii) support another party's case; and
>
> (c) the documents which he is required to disclose by a relevant practice direction.

There is a duty of search in respect of standard disclosure that is set out in Civil Procedure Rule 31.7, which provides:

> (1) When giving standard disclosure, a party is required to make a reasonable search for documents falling within rule 31.6(b) or (c).
>
> (2) The factors relevant in deciding the reasonableness of a search include the following–
>
> (a) the number of documents involved;
> (b) the nature and complexity of the proceedings;
> (c) the ease and expense of retrieval of any particular document; and
> (d) the significance of any document which is likely to be located during the search.
>
> (3) Where a party has not searched for a category or class of document on the grounds that to do so would be unreasonable, he must state this in his disclosure statement and identify the category or class of document.

[56] http://www.cps.gov.uk/legal/section20/chapter_g.html

The rules were largely conceived on the basis that the “documents” would be in paper form. A recent report from a working party chaired by Mr Justice Cresswell has reviewed the position and come up with a series of recommendations[57]. In any event, the report indicates a number of practical routes that can be followed, irrespective of the need to change the rules or associated guides and practice directions. It includes a draft suggested revision to the existing Commercial Court Guide.

[57] Http://www.courtservice.gov.uk/cms/media/electronic_disclosure1004.doc

## Appendix 6: Problems of Obscene and Indecent Material

Human beings are interested in sex, and in some cases this takes the form of accumulating and sometimes distributing quantities of pictures with extreme sexual content. In a corporate environment this may be the subject of a specific inquiry or may be discovered during an entirely separate investigation.

This appendix explains the main problems that corporate investigators may encounter and the risks to - and obligations of - the organisation.

English law distinguishes between adult and child pornography and also between material which is "obscene" and that which amounts to "extreme pornography". For this purpose a "child" is someone who is or appears to be under the age of 18 (s. 45 of the Sexual Offences Act 2003).

In terms of adult material the test of obscenity is applied by a court. Section 1(1) of the Obscene Publications Act 1959 states:

> (1) For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

In practice over the years, juries have become steadily more permissive and the prosecution criteria have tended to move in step. There is no offence in possessing such material, only if it is "published". The test for publication is:

> (3) For the purposes of this Act a person publishes an article who–
> (a) distributes, circulates, sells, lets on hire, gives, or lends it, or offers it for sale or for letting on hire; or
> (b) in the case of an article containing or embodying matter to be looked at or a record, shows, plays or projects it [, or, where the matter is data stored electronically, transmits that data].

The Crown Prosecution Service tends to want strong *prima facie* evidence of publication for gain, widespread offence being caused by virtue of public display, or ease of access.

After January 2009 there will be a new offence of possession of "extreme pornographic images" in the Criminal Justice and Immigration Act, 2008, section 63[58]. Extreme pornographic images have a narrower definition than "obscene" for the purposes of the Obscene Publications Act. The test is:

[58] http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_9#pt5-pb1-l1g63

> (7) An image falls within this subsection if it portrays, in an explicit and realistic way, any of the following—
>
> (a) an act which threatens a person's life,
>
> (b) an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals,
>
> (c) an act which involves sexual interference with a human corpse, or
>
> (d) a person performing an act of intercourse or oral sex with an animal (whether dead or alive),
>
> and a reasonable person looking at the image would think that any such person or animal was real.

This is a "strict liability" offence. Strict liability means that there is enough to convict, provided that a person is found in possession of offending material and that they know that they are in possession. There are a small number of defences, which the defendant has to prove to the court on the balance of probabilities. Further guidance, published by the Ministry of Justice in November 2008, is available at: http://www.justice.gov.uk/docs/extreme-pornographic-images.pdf

Child material is dealt with under the Protection of Children Act 1978 which creates offences of "making" and "distributing" an indecent image of a child under the age of 18. The Court of Appeal has interpreted "making" to include the simple "making of a copy" or even "causing a picture to appear on screen knowing that it was indecent". An important extension of the 1978 Act exists within s. 160 of the Criminal Justice Act 1988. The effect of s. 160 of the Criminal Justice Act 1988 is that, as with extreme pornography, it is a "strict liability" offence to possess "indecent" pictures (i.e. of children in a sexual situation).

The combination of the strict liability offence of "possession" and the tight definition of "making" have the potential to create significant difficulties for the organisation or corporate investigator, who just wants to do the right thing.

Section 46 of the Sexual Offences Act 2003 provides a defence that a "making" was necessary to do so for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings. Section 46 works on a "reverse burden of proof" basis. A defence is available where a person "making" such a photograph or pseudo-photograph can prove that it was necessary to do so for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings. A memorandum of understanding between the Crown Prosecution Service and the Association of Chief Police Officers dated 6 October 2004 provides guidance[59]. It seeks to protect those who genuinely come across such

[59] See http://www.cps.gov.uk/publications/docs/mousexoffences.pdf

material unexpectedly but may be called upon to preserve evidence, while discouraging amateur sleuths, bogus “researchers” and vigilantes.

The factors affecting the decision whether to accept a claim that “making” was covered by the s 46 defence are:

- the way in which the indecent photograph or pseudo-photograph was discovered or made – those knowingly making abusive images will need to demonstrate that they have some identified role or duty, as a result of which they needed to respond to a complaint, investigate the abuse of a computer or other electronic communications system, or access particular data, and that they “made” the images within the course of that duty;
- the speed with which the indecent photograph or pseudo-photograph was reported and who it was reported to;
- the handling and storage of the indecent photograph or pseudo-photograph –whether it was appropriate and secure;
- that the copying of photographs or pseudo-photographs must be the minimum to achieve the objective and be appropriate;
- that individuals should be expected to have acted reasonably.

A further bit of advice is that it is prudent that all decisions made by a system administrator and an organisation that finds itself unexpectedly handling indecent material should keep careful and full records in internal minutes.

In due course it is likely that new guidance will be issued to cover the handling of extreme pornography under s 63 of the Criminal Justice Act, 2008 but for the moment it seems sensible to make the ACPO/CPS Guidance on indecent images of children also apply to extreme pornography. Indeed the defences available under the 2008 Act track closely those in s160 of the Criminal Justice Act 1988 which covers possession of indecent images of children. For the moment the only specific official help is to be found in the Ministry of Justice document referred to above.

The Internet Watch Foundation (http://www.iwf.org.uk) is the only non-police body to whom suspected indecent material can be reliably and readily reported. The website contains, among other things, a form for reporting and various items of advice for IT professionals as well as an explanation of its other activities. It was formed in 1996 following an agreement between the government, police and the Internet Service Provider (ISP) industry that a partnership approach was needed to tackle the distribution of child abuse images online. It operates the only authorised hotline in the UK for the public to report their inadvertent exposure to illegal content on the Internet. It is funded by the EU and UK Internet industries, including ISPs, mobile network operators and manufacturers, content service providers, telecoms and software companies and credit card bodies.

## Appendix 7: Encryption Issues

Although during the course of an internal investigation a business may come across material encrypted by a suspect, since October 2007 UK businesses have needed to plan for another sort of eventuality: where they themselves use encryption to protect files and communications traffic and are asked by law enforcement to produce material in “intelligible” form.

There are three main circumstances in which encrypted material is found in corporate investigations:

- The organisation itself uses encryption facilities in the course of its business. In these circumstances the solution to decrypting often lies in the hands of the organisation. However there may be obligations to third parties, such as customers or clients etc). However some organisations use encryption the passphrase for which changes with each session, but this usually applies to encryption used in the course of transmitting data rather than for stored files
- Where an individual has used encryption for their own use and outside any corporate framework
- When law enforcement in the course of an investigation requests access to information that would normally be held in encrypted form

***Decryption techniques:***

It is beyond the scope of this guide to deal in any detail with methods of decrypting encrypted files, but it may be helpful to understand some of the basic steps an investigator will follow

The first step is to seek to identify the specific encryption product deployed. This can usually be done by searching the associated PC – at the very least there has to be software or hardware capable of encrypting and decrypting. The next step is to determine the unique passphrase. There are a variety of methods; some encryption systems have turned out to be inherently weak so that the vulnerabilities can be exploited by specific software tools – many of these are available on the web. A second approach is to use the so-called “dictionary attack” where a list of large numbers of “typical” passwords are thrown at the encrypted file until one of them works.

If a disk which contains encrypted files is examined forensically it is sometimes possible to locate file fragments which are either of the cleartext versions of the encrypted files or are the passphrases. The “dictionary attack” and “forensic examination” methods can also be combined: once a disk (with all its deleted content) has been forensically examined its entire contents can be indexed and each word in the index added to the “dictionary” – the theory being that if the passphrase exists on the disk somewhere it will eventually be fed to the encrypted file and decrypt it.

### *Powers to compel decryption*

Powers to make it a criminal offence not to provide plaintext versions of encrypted material, or the means by which encrypted material can be decrypted were introduced into the Regulation of Investigatory Powers Act in 2000 (in Part III), but the relevant sections were nor brought into force until 2007. It took until then for a number of misgivings from the banking and computer industries to be addressed.

Although foremost is the minds of legislators was the situation of the individual PC owner with a requirement for concealment – typical examples would be those planning terrorist attacks and collectors of pictures of child sexual abuse – the legislation also covers organisations that store and transmit encrypted information.

The main concerns these had were:

- That law enforcement would demand encryption keys which rendered into plaintext not only the material covered by a warrant but other, innocent files, including those which the organisation held in confidence
- That some encryption methods, particularly those used to transmit data, involve the use of ever-changing session keys. As a result at any one time the organisation would not know the key in use; the only way to provide decrypted access to law enforcement might be to drop encryption altogether
- That they might receive an Order which while valid nevertheless involved great cost and inconvenience and there would no way to negotiate an alternative

The main relevant provisions of RIPA are:

- power to require disclosure of protected information in an intelligible form (section 49);
- power to require disclosure of the means to access protected information or the means to put it into intelligible form (section 50(3)(c); and
- power to attach a secrecy provision to any disclosure requirement (section 54).

In order to allay the anxieties of organisations, a Code of Practice has been issued: *Investigation of Protected Electronic Information* [60]

Public authorities seeking access must fulfil a number of requirements – for example notices can only be issued by a restricted group of office holders, the information sought must be identified as specifically as possible, all orders must satisfy necessity and proportionality tests, explanations must be provided, and there should be circumstances allowing the recipient of such a notice to discuss the precise means of compliance – for example what information is actually needed in order to satisfy the needs of an investigation.

[60] http://security.homeoffice.gov.uk/ripa/encryption/

The Code of Practice lays great emphasis on attempting to achieve a consensus and in particular that an organisation or individual served with such an order be allowed to supply the protected information in an unprotected format rather than supplying the key that would perform the decryption.  This would be particularly important where the key opens up documents which are not relevant to the enquiry.

For businesses the problem remains that there may be a clash between existing obligations of confidentiality and the receipt of an order to decrypt.  In those circumstances lawyers may advise a business to wait until there is judicial order which they can say they were compelled to comply with.

## Appendix 8: UK Law Enforcement Resources and Structures

The current position for a business that wishes to report a computer-related crime to UK law enforcement is not straight-forward. However at the end of September 2008 the Home Office made announcements and provided funding for units that should come into existence in the first half of 2009.

The plan is as follows. All local police forces now have some capacity to handle computer disk and network forensics, although the latter is limited to networks which follow internet-like (TCP/IP) protocols. In some forces the specialists are all police officers but others employ civilians; in addition there are a number of private companies, usually staffed by ex-law enforcement personnel, which provide technical support. Overall the coverage is best described as “patchy”. There are a number of specialist police officers possessed of considerable skill and some of these have Masters’ degrees in digital forensics. But equally some of the officers within local hi-tech crime units may only have been involved in the area for a very short time and only received quite limited specialist training.

From Spring 2009 there will be a new Police Central e-crime unit (PCeU) which will provide specialist officer training and co-ordinate cross-force initiatives to “crack down on online offences”.[61] It will be based at the Metropolitan Police and is part-funded by the Met and the Home Office.

It will need to interact with other new initiatives: there are to be a National Fraud Reporting Centre, National Fraud Intelligence Bureau and a National Fraud Strategic Authority[62]. The City of London Police is the lead force for fraud.

The Metropolitan Police currently has several semi-separate units dealing with computer evidence, not only the Computer Crime Unit but also specialist entities to assist in Special Branch, anti-terrorism and child protection. It also has a specialist civilian-staffed Computer Systems Laboratory to conduct examinations of computers, PDAs and cellphones. The City of London Police’s unit concentrates on fraud and has close contacts with financial institutions and regulators. It has a Cheque and Credit Card Fraud Investigation Unit[63].

The Ministry of Defence Police is charged with the security of defence sites and events in and around them, as opposed to issues of pure military discipline. It has the largest fraud squad in the UK and that includes a computer forensics unit[64].

SOCA[65], the Serious Organised Crime Agency, came into existence in 2006 and was formed from the old National Crime Squad, National Criminal Intelligence Service and elements from Customs and Revenue and the Security Service. It describes itself as “an intelligence-led agency with law enforcement powers and harm reduction responsibilities. Harm in this context is “the damage caused to people and

[61] Home Office press release 30 September 2009

[62] Hansard 19 June 2008; http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080619/text/80619w0005.htm#08061980001736

[63] http://www.cityoflondon.police.uk/NR/rdonlyres/3528E395-EDE9-4B8C-A8BA-829C00982E0D/0/chequecreditcardfraudinvestigationFOI.pdf

[64] http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/MDPGA/AboutMinistryofDefencePolice.htm

[65] http://www.soca.gov.uk/

communities by serious organised crime." Its main pre-occupations are trafficking of Class A drugs and organised immigration crime and fraud; it also deals with the confiscation of assets which are the results of crime and the Suspicious Activity Reports issued by banks to counter money-laundering. It has an E-Crime Unit which supports all of these activities but which also investigates large-scale hi-tech crime. SOCA is an "Executive Non-Departmental Public Body" sponsored by, but operationally independent from, the Home Office and is not directly "police". Much of its work tends to avoid too much publicity though the E-Crime Unit takes part in publicity drives about computer security as part of its "harm reduction" remit.

The Serious Fraud Office (SFO)[66] investigates and prosecutes serious or complex fraud. It is responsible to the Attorney-General. It started work in 1988 and has been through a series of revisions of its detailed remit. Not the least of its difficulties is that complex fraud requires lengthy and expensive investigations and trials are correspondingly long and costly. For as long as it has been in existence critics have wondered how far cases could be simplified and how far the penalties could extend beyond the obvious criminal sanctions of fines and imprisonment to regulatory controls, in effect to stop fraudsters from trading. The SFO has strict acceptance criteria for the sorts of case it takes on:

- does the value of the alleged fraud exceed £1 million?
- is there a significant international dimension?
- is the case likely to be of widespread public concern?
- does the case require highly specialised knowledge, e.g. of financial markets?
- is there a need to use the SFO's special powers, such as Section 2 of the Criminal Justice Act?

The SFO has a specialist computer forensics unit and also has significant expertise in handling large quantities of evidence in both paper and electronic form

CEOP[67], the Child Exploitation and Online Protection Centre, is part of the UK police service but also has links to SOCA. Its main function is the protection of children against sexual abuse, but it also has an investigation and enforcement unit which has significant technical expertise.

The Home Office hopes that all these units will work together harmoniously.

Specialist units within HM Revenue and Customs, Benefits Agency and Department of Trade and Industry continue to grow.

The National Technical Assistance Centre (NTAC) handles warranted intercepts under the Regulation of Investigatory Powers Act 2000 and also acts as the central law enforcement resource for handling encrypted data. It is staffed predominantly by law enforcement officers but is not part of the UK police service,

The Association of Chief Police Officers (ACPO) encompasses a Computer Crime Working Group. A *Good Practice Guide for the Handling of Computer Evidence* is published by ACPO. The Working Group works closely with the Home Office Digital Evidence Group, which has representatives from all law enforcement agencies and the Crown Prosecution Service.

[66] http://www.sfo.gov.uk/

[67] http://www.ceop.gov.uk/

The Forensic Science Regulator[68] is a “public appointee” sitting in the Home Office whose function is to ensure that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards. The Regulator has been in place since the beginning of 2008 and has set up an advisory specialist group to deal with digital evidence,

In the private sector, some large telecoms companies, including ISPs, have set up their own investigatory and specialist forensic units, not only to address fraud against themselves but to service the requirements of law enforcement under the Regulation of Investigatory Powers Act 2000; a system of Single Point of Contact (SPOC) has been set up to streamline the process and develop consistent standards. A number of organisations support the anti-piracy initiatives of the trade associations for owners of intellectual property, e.g. Federation Against Software Theft, Business Software Alliance, Entertainment and Leisure Software Publishers Association; often their staff are drawn from law enforcement and Trading Standards.

There is thus some significant capacity within the UK to tackle e-crime but critics have complained that there has been insufficient co-ordination of initiatives and resources.

/[68] http://police.homeoffice.gov.uk/operational-policing/forensic-science-regulator

# Appendix 9: Good Practice Guidance – National and International Standards for Records Management

In addition to guidance on the handling of computer-related evidence further "good practice" advice can be found in the International Standard on Records Management – ISO 15489 and the related British Standard BS10008:2008.

ISO 15489 is for any organisation that needs to ensure that its records (both paper and electronic) are properly maintained, easily accessible and correctly documented from creation right through to ultimate disposal, be it archiving, imaging or destruction. The standard ensures that disposal is carried out in a transparent manner according to pre-determined criteria. ISO 15489, which emerged from work done by the British Standards Institute (BSI) in the 1990s (Code of Practice on 'Legal Admissibility and Evidential Weight of Information Stored Electronically'- BSI PD0008), is directly aimed at organisations that need to reassure customers and clients that they maintain accurate, detailed records according to a stated policy, for example, the health, financial services and state-funded sectors.

In its earliest form the Standard addressed a technology known variously as document management systems or electronic records management. Many organisations were scanning important paper documents – mortgages, insurance policies, cheques, etc. – and placing them on optical media (in the mid-1990s this was on so-called Write Once Read Many - WORM media) so that they could be stored and retrieved efficiently and economically. The immediate problem was to take proper steps to ensure that the results would be regarded as both reliable and admissible in court. BSI PD0008[69] provided high-level guidance and the detail came in a workbook, PD0009[70].

The updated and international version appeared in 2001 as ISO 15489[71]. The Standard provides a descriptive benchmark that organisations can use to assess their record-keeping systems and practices. The two parts of the Standard are designed to help organisations create, capture and manage full and accurate records to meet their business needs and legal requirements, as well as to satisfy other stakeholder expectations. Both parts apply to records in any format or media that are created or received by any public or private organisation during the course of its activities.

Part 1 provides a high-level framework for record-keeping and specifically addresses the benefits of records management, regulatory considerations affecting its operation and the importance of assigning of responsibilities for record-keeping. It also discusses high-level records, management requirements, the design of record-keeping systems and the actual processes involved in records management, such as record capture, retention, storage, access, etc. For example, conventional "computer security" and audit practices are important components because it is essential to be able to demonstrate beyond doubt that data has not been altered at any stage. Part 1 concludes with a discussion of records management audit operations and training requirements for all staff of an organisation.

[69] Code of Practice for Legal Reliability and Evidential Weight of Information Stored Electronically, available at: http://www.bsi-global.com/ICT/Legal/bip0008.xalter

[70] See http://www.bsi-global.com/ICT/Legal/bip0009.xalter

[71] Http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31908&ICS1=1

Part 2 provides practical and more detailed guidance about how to implement the framework outlined in Part 1.  For example, it provides specific detail about the development of records management policy and responsibility statements.  Part 2 also provides practical guidance about the development of records processes and controls and specifically addresses the development of key record-keeping instruments such as thesauri, disposal authorities and security and access classification schemes.  It then discusses the use of these tools to capture, register, classify, store, provide access to and otherwise manage records.  Further, Part 2 provides specific guidance about the establishment of monitoring, auditing and training programmes to promote and effectively implement records management within an organisation.

BS10008, which is specific to the UK, appeared in November 2008. It claims that compliance "ensures that any electronic information required as evidence of a business transaction is afforded the maximum evidential weight. The process is based on the specification of requirements for planning, implementing, operating, monitoring and improving the organization's information management systems".  It is a consolidation and updating of the work commenced under PD0008.[72]

Compliance with a national or international standard, even the production of a certificate of compliance, does not automatically make records produced from such a system admissible, but it does provide a great deal of comfort.  BS10008 is specifically referred to in the Code of Practice issued under s. 46 of the Freedom of Information Act 2000, which lays down rules for all public bodies that are likely to be called upon to produce their records. (Appendix 2 lists out some of the main types of digital evidence and the problems likely to be encountered when seeking to acquire and preserve them.)

[72] http://www.bsigroup.com/en/Shop/Publication-Detail/?pid=000000000030172973#5

# Appendix 10: Additional Resources

### *Statistics and Forecasts About the Future of Cybercrime*

Many published surveys can be dismissed because the survey sample is too small or unrepresentative. However, the following detailed studies are worth examining:

- *Cyber Trust and Crime Prevention* – a study by the Home Office and the Department of Trade and Industry Foresight Team: http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html
- *The Future of Netcrime Now* – a Delphi study by the Home Office: http://www.crimereduction.gov.uk/internet01.htm
- *Audit Commission ICT Fraud and Abuse Survey* – http://www.audit-commission.gov.uk/
- Computer Security Institute / Federal Bureau of Investigation Computer Security Survey – http://www.gocsi.com/

### *Risk Management and Information Security*

The international standard for Information Security Management is ISO 17799, which is based on BS 7799, available from http://www.bsonline.bsi-global.com/server/index.jsp.
CPNI publishes a guidance document, *Risk Management and accreditation of information systems*, which is also HMG Infosec Standard No 2. It is available for download from http://www.cpni.gov.uk/docs/re-20050804-00653.pdf

### *Computer Security and Incident Response Teams*

Evidence collection is likely to be an aspect of other corporate activities. It could be one of the functions of a Computer Security and Incident Response Team (CSIRT).

A CSIRT is a service organisation that is responsible for receiving, reviewing and responding to computer security incident reports and activity. Its services are usually performed for a defined constituency that could be a parent entity such as a corporation, government or educational organisation, region or country, research network or paid client.

Part of a CSIRT's function can be compared in concept to a fire department. When a fire occurs, the fire department is called into action. They go to the scene, review the damage, analyse the fire pattern and determine the course of action to take. They then contain the fire and extinguish it. This is similar to the reactive functions of a CSIRT.

A CSIRT will receive requests for assistance and reports of threats, attack, scans, misuse of resources or unauthorised access to data and information assets. They will analyse the report, determining what they think is happening and the course of action to take to mitigate the situation and resolve the problem.

Just as a fire department can be proactive by providing fire-prevention training, instructing families in the best manner to exit a burning building safely and promoting the installation of smoke alarms and the purchase of fire escape ladders, a CSIRT may also perform a proactive role. This may include providing security awareness training, security consulting, configuration maintenance and producing technical documents and advisories.

A good starting point is: http://www.cert.org/archive/pdf/03tr001.pdf. The websites http://www.cert.org and http://www.first.org provide a wide range of advice.

Guidance for "First Responders" can be found at:
http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

### *Computer Forensic Analysis Tools*

The following are some of the better-known products. It is not possible to make effective use of them without proper training. Because of the rate of change in ICT, products can rapidly become obsolete unless there are frequent new versions. Most experienced digital forensic investigators will use a variety of tools.

*Disk imaging and analysis*

- EnCase (http://www.guidancesoftware.com)
- AccessData FTK (http://www.accessdata.com)
- ProDiscover (http://www.techpathways.com)
- Sleuthkit and Autopsy (http://www.sleuthkit.org/)
- SMART (http://www.asrdata.com/index.html)
- Ilook (Law enforcement only) http://www.ilook-forensics.org/
- Blackbag (for Apple Mac) (http://www.blackbagtech.com/products.html)
- MacForesnsicsLab http://www.macforensicslab.com/
- Paraben (also for PDAs) (http://www.paraben-forensics.com/)
- Tucofs – website listing many tools (http://www.tucofs.com/tucofs.htm)
- Open Source tools (http://www.opensourceforensics.org/)

A Google or other search on "computer forensics" and "forensic computing" will yield many websites, articles, courses, training schemes and conferences.

## Glossary of Terms Used in Digital Evidence

| | |
|---|---|
| ACPO Guide | The Association of Chief Police Officers' *Good Practice Guide to Computer-based Evidence* |
| ActiveX | A Microsoft programming device used on websites, for example to create fillable forms or animations |
| application | A computer program |
| attachment | A file of any kind linked to an email, newsgroup posting, etc. The attachment may usually be in any of a number of formats |
| audit trail | A record of activities in chronological form |
| backdoor | A facility, in either software or hardware, which enables security and authentication mechanisms to be circumvented |
| back-up | A regular process to create additional copies of essential data and programs, or indeed entire systems. Back-up may be either complete or partial and, on each occasion, may be complete or incremental |
| BIOS | Basic Input–Output System. More colloquially BIOS refers to the hardware chip on a computer that runs on start-up and "looks for" a disk with a full operating system. The BIOS contains the system clock and may contain details of additional hardware installed on the computer. Although they are not identical, sometimes also referred to as CMOS (see *CMOS*) |
| bot | A robot program used to perform a particular function, for example, to keep a transmission channel artificially open or to send out rogue commands. A bot army or botnet is a collection of bots on different computers working in concert. Innocent third-party computers taken over in this way are referred to as zombies. May be used for "phishing" or denial of service (DOS) attacks |
| browser (or web browser) | A program used to view the world wide web, such as Internet Explorer, Netscape, Mozilla, Firefox, Opera, Safari |
| brute force | A common technique to break a password system by writing a program to throw large numbers of potential passwords exhaustively at a computer in the hope of eventually finding the correct one |
| cache | A holding area for temporary files, often used to speed up regular computer processes. The best known example is the Internet cache which contains recently viewed webpages and pictures |
| CERT | Computer Emergency Response Team |
| chatroom | An Internet facility to enable participants to talk online by typing on the keyboard. It occurs in real-time (see *newsgroups*) |
| CMOS clock | A battery-driven device which is the main source for the day and time data associated with each file (see *BIOS*) |
| communications data | In English law, "communication" is information about who is connected to who, when and for how long, but not including the content of the communication. Traffic data is a subset (see Traffic Data). |
| configuration file | A file normally hidden on a computer that affects the specific way in which an individual program, hardware accessory or entire computer works. On Windows machines, it is often identified by the extension ".ini" (INI files) |

cookie A small text file installed and stored on a computer by a website so that it can track a user's activities and welcome them on a return visit

cryptography Method used to hide the contents of a file, etc. (see *Encryption*, *Steganography*)

CSIRT Computer Security Incident Response Team

day and time stamps Day and time information from an on-board computer clock. All modern operating systems associate with each file a series of day and time stamps, although there are variations.

denial of service (DOS) attack An attack on an Internet site which involves sending large numbers of messages to that site to overwhelm and prevent it from operating properly

dictionary attack A common technique to break a password system by writing a program to throw large numbers of "likely" potential passwords at a computer

digital fingerprint A technique for uniquely identifying identical files (see *hash*)

directory A hierarchical system of organising files in places where they can be easily found on a computer hard disk (also known as folders)

disclosure The legal process by which information is fairly made available to opposing counsel and which is subject to a number of rules and obligations (known as "discovery" in the US)

disk acquisition A process to make an accurate exact copy or "image" of a hard disk, CDROM or other data memory device, creating an intermediate file which can be examined using specialist tools and from which clones of the original can be created

distributed denial Using large numbers of computers to attack and overwhelm a target

of service (DDOS) attack computer (see *denial of service (DOS*) *attack*)

DNS Domain Name Server. An essential element of the Internet – a constantly updated collection of computers that translates the name of a computer into its IP address

DNS poisoning Attacking a DNS so that requests to one website are redirected to another rogue site

dongle Hardware device, usually connected to a USB or printer port, sometimes used to provide encryption protection to computers, without the dongle the disk can't be "read". Also used as a counter-piracy measure – the dongle is required to make a particular high-value program "run".

DOS (1) Disk Operating System. Windows, Unix, Linux, MacOS, Solaris, OS/2 and VMS are all operating systems for various items of computer hardware.

DOS (2) MS-DOS, the Microsoft disk operating system which was common before Windows 95

dynamic IP address An IP address assigned on an as-needed basis. Over a period of time an individual may use several IP addresses from the same range within the user's Internet Service Provider (ISP) (see *IP address*) email server A computer that manages the distribution and reception of email on behalf of a community of users, holding mail until an individual is ready to download it

EnCase Popular forensic computing suite which is capable of imaging a hard disk and then analysing it

encryption The translation of files, data, pictures, etc. into a form in which it can only be read/viewed by those authorised to do so. Encryption requires an algorithm (generic method) a key which is only known to participants. In conventional encryption the same key is used by both sender and recipient. Encryption, together with an appropriate management system, can also be used to authenticate documents

expert evidence In English law, opinion evidence from someone whom the court has decided to accept as an expert (see *technical evidence)*

false positive Where a system has raised an alarm which on inspection turns out to be misplaced

FAT, FAT32 The Microsoft disk operating system used in MS-DOS and Windows 95, 98, etc. The FAT table contains information about the specific physical locations on disk of files (which may be fragmented) and is also the source of date and time stamp data (see *NTFS*)

file compression A technique for reducing the size of a file to make it smaller to transmit or store. In “lossless” compression, no original data is lost but many compression schemes involve an “acceptable” level of loss. ZIP, RAR, tar and Stuffit are general-purpose file compression schemes, MP3 is particular to sound files (see *ZIP*)

file-sharing program A system to enable many people to share files. These files may have an “illegal” element because they violate copyright or are indecent. In order to participate in a file-sharing system, a user may require specialist client software

file signature A specific series of computer characters at the start of the internal structure (or format) of a file which helps computer applications identify the file.

firewall Security device for internet-connected computers that is able to limit inbound and outbound traffic. The best firewalls are separate hardware units, although software firewalls exist and can provide a degree of protection

folder See *directory*

format (1) of a disk – the creation of an internal structure so that it can hold files. Reformatting consists of replacing an existing scheme with a new one, which renders the old files difficult to read and recover without the use of advanced techniques

format (2) of a file – each computer application creates and reads files with a specific internal structure, known as format

FRP Forensic Readiness Program

GSM tracking Service which pinpoints the location of an individual or vehicle via signals exchanged between a cellphone handset and base stations

Gb Gigabyte. A unit of capacity of data or memory (1 Gb = 1024 Mb) hash See *digital fingerprint*

hash analysis/ hash libraries Libraries exist of digital fingerprints for well-known files, for example those associated with popular operating systems and programs and offensive material. They can be used to scan hard disks rapidly to eliminate files of no interest or to look for files of particular significance

hot-firing The process by which a clone of an original file is placed in suitable hardware so that what the original user saw can be viewed. The usual result is that data on the hard disk becomes altered and re-cloning may be necessary during an extended examination

HTML Hypertext Mark-up Language. The language used for creating webpages containing not only content but formatting and other instructions. Many browsers contain a "View Source" option so that code can be viewed easily.

HTTP Hypertext Transmission Protocol. The protocol of the World Wide Web. HTTPS is a secure version used for e-commerce transactions, etc.

IDS Intrusion detection system – in effect, a burglar alarm for computer systems

image (1) A file containing a photograph or a picture

image (2) The process of making an entire copy of data media such as a hard disk. Some "imaging" programs" are designed to aid data recovery or to support the needs of a large organisation

Internet Relay Chat (IRC) The international protocol for online chatting. Other web interfaces can be used (see *chatroom*)

IP address A uniquely identifiable, machine readable, number for each computer or host, on the Internet, that can be used by the Internet Protocol to transmit and receive traffic. Servers, websites and other computers permanently connected to the Internet always have the same, static IP address. Many ISPs allocate users an IP address on an as needed basis – this is known as a 'dynamic IP address' as it can change within a range set by the ISP. Over a period of time an individual may have used several IP addresses from within one range.

IP spoofing A technique for altering or compromising an IP address so that it appears be a third party

ISP Internet Service Provider. A business or other organisation that links individual users to the Internet and that also provides other associated services such as email management and web space

Java A programming language frequently used on websites, for example to create online forms or animations

jumper A small connector on a hardware device such as a motherboard or disk drive. The connector links one or more protruding pins and makes the hardware behave differently, for example, to order which of two hard disks has priority – "master" or "slave"

Kb Kilobytes. Unit of capacity of data or memory (1024 Kb = 1 Mb)

keystroke monitor/ A covert program which captures every keystroke that a computer keylogger user makes so that they can be examined later. Hardware-based keyloggers exist as well; they are usually physically very small and are placed in-line to a computer's keyboard; PS/2 and USB connection versions ate available. Keyloggers can be used to identify passwords and the software versions may be part of a Trojan. But keyloggers may also be deployed for investigatory surveillance purposes

Linux Popular operating system, part of the Unix family. They are typically released in working "distributions" or "disros" such as SUSE, Red Hat, Unbuntu, Debian, etc

logic bomb Rogue program with a delayed effect which causes damage to data. It may be triggered by time or some external event

macro An automated sequence of computer commands

Mb Megabyte. Unit of capacity of data or memory (1024 Kb = 1 Mb)

meta-data Literally, data about data. Some regular computer files contain hidden additional information which can be viewed

newsgroups Internet-based discussion groups, one of the oldest Internet "institutions", where participants post messages for later viewing. It can be used to publish attached files (also known as Usenet)

NTFS The Microsoft Disk Operating System used in Windows NT, 2000 and XP, A replacement for FAT and FAT32. The MFT (Master File Table) contains information about the specific physical locations on disk of files (which may be fragmented) and is also the source of date and time stamp data

Open Source Computer programs which are written on a "community" basis and are usable without restriction (also known as "freeware"). They may need to be adapted to work well in specific circumstances

packet The quantity of data sent over a network. Both for efficiency and to allow for error-checking, files are split up into packets for transmission and then re-assembled in the correct order on reception. "Packet switching" is a data transmission technique to maximise the efficient use of physical cables, satellite links, etc.

packet filtering A technique for listening on a data transmission and selecting packets according to particular criteria

packet sniffer The device that listens for data transmission (see *packet filtering*)

partition A means of dividing a hard disk so that it presents itself to the operating system as one or more hard disks (e.g. C:, D:, etc.). The technique separates programs from data files and makes back-up easier; it makes one or more operating systems available on the computer; and it maintains an area containing recovery files. Partitions can also be hidden

payload The "bomb" or result of a logic bomb or virus

PDH Pleas and directions hearing. An increasingly important procedure in the English criminal justice system where, prior to a trial, discussions take place about its length, numbers of witnesses, arrangements for experts, dates, etc.

phishing Creating temporary fake websites to incite visitors to release sensitive information for fraudulent purposes. Usually, users are lured to the fake websites via emails purporting to come from legitimate sources such as banks

phreaking The abuse of telephone and similar systems

pop-up Subsidiary windows which appear on the screen during Internet use. These may contain detail related to the main window or for advertising

port Exit and entry points to a computer system. Internet communications protocols designate a number of ports to a computer system; certain ports always have the same function (port 80 is used for websites, for example). All ports on a computer which are not going to be used should be closed off (see *firewall*)

port scanner A program which looks for “open” ports – in malicious scanning, leading to computer intrusion and possible abuse

protocol A set of rules enabling computers and electronic devices to exchange data, etc. in an agreed, pre-defined way

proxy A device or program that performs an operation while hiding the details from outside scrutiny

PKI Public Key Cryptography - a more sophisticated version, where there are large numbers of participants to a system, different (paired) keys are used for encryption and decryption – public key cryptography. Encryption, together with an appropriate management system, can also be used to authenticate documents

RADIUS Remote Authentication Dial In User Service – a log maintained by many ISPs to record who had the use of a specific dynamic IP address at a given time

registry In modern Windows systems, a normally hidden part of the operating system that holds important configuration and other data

root The operating system at its most fundamental level of control

root kit A series of rogue programs used to take control of an operating system

serialing An ascending unique serial number assigned in situations where a system is recording transactions, so that any attempt at transaction deletion can be seen

server A program that sits on a network (including the Internet) waiting to respond to requests (see *email server* and *web server*)

spidering A technique for capturing a website – the program identifies all the internal links on a page and follows them through. Spidering can only capture fixed pages, not ones which are dynamically created

steganography A techniques for hiding data in an apparently innocent file

swap file When a computer runs out of memory on its motherboard during use it will “swap” data to the hard disk. The swap file sometimes contains a record of recent activity on the computer

Tb Terabyte. Unit of capacity of data or memory (1 Tb = 1024 Gb)

TCP/IP Transmission Control Protocol / Internet Protocol. The set of networking protocols used on the Internet and on some private networks

| | |
|---|---|
| technical evidence | Evidence which is the result of a specific technical procedure or investigation; “expert evidence”, on the other hand, as far as the courts are concerned, can include the opinion of the witness |
| thumbdrive | A small portable hard disk drive, usually with a Universal Serial Bus adaptor |
| Tracert (traceroute) | A program used to identify all the links between a computer and the one to which it is connected |
| Traffic Data | explanation… |
| Trojan defence | A claim by a defendant that they are not responsible for activities apparently associated with their computer. The counter to the Trojan defence is to search the defendant’s computer for signs of a rogue program (see *Trojan horse*) |
| Trojan horse | A hidden program which covertly opens a port on an Internet-connected computer, enabling the contents of that computer to be viewed and altered and the whole computer to be remotely controlled. To work, the Trojan needs a “server”, which is installed on the target computer; and a “client”, which the perpetrator uses to send out commands |
| Unallocated space | Files or fragments of files that do not have an associated entry in an index on the hard disk but are still physically present. Very often they have missing or incomplete date or time stamps. Also known as material from unallocated clusters. |
| Unix | Family of operating systems which includes GNU-Linux, Solaris, BSD Unix and many others |
| URL | Universal Resource Locator – the address of a site or file on the world wide web |
| user profiles | On more sophisticated computer operating systems, a profile of each user with their own desktops, programs, etc, accessed via a separate username and password. The most important user profile is that of the Administrator, who may have complete control of and access to the computer |
| virus | A self-replicating malicious program. There are many specific definitions that distinguish a virus from a worm (see *worm*) |
| war-driving | The technique of driving around in a motor vehicle looking for open, unprotected wireless networks |
| web server | A program holding webpages that will be sent on specific request |
| whois | An internet facility to find out who owns an IP address or website |
| worm | A self-replicating malicious program (see *virus*) |
| write-protect | A hardware or software device used to prevent inadvertent alteration of an original disk |
| ZIP | A file compression program. A zip file contains one or more compressed files |
| ZIP disk | Larger capacity removable disk medium |
| zombie | A third-party computer utilised in a distributed denial of service (DDOS) attack (see *Denial of service (DOS)*) |

# Information Assurance Advisory Council

# IAAC

## SPONSORS

AIRWAVE

UNISYS
imagine it. done.

Anite public sector

BT

NORTEL

symantec.

Microsoft

RSA SECURITY

## MEMBERS, GOVERNMENT LIAISON PANEL

CESG

csia
Central Sponsor for Information Assurance

CPNI
Centre for the Protection of National Infrastructure

BERR
Department for Business Enterprise & Regulatory Reform

SOCA

**For more information on IAAC please contact:**

Information Assurance Advisory Council (IAAC)
North Star House
North Star Avenue
Swindon SN2 1FA
United Kingdom
T:+44(0)1793417453
E: info@iaac.org.uk

**www.iaac.org.uk**