

# **Ibas Computer Forensics**

## **A White Paper**

**by Simon Janes**

### **Introduction**

This paper has been prepared as background information and analysis relating to the drivers and benefits for the provision of a professional response to computer related incidents.

The evolution of Information and Communication Technology (ICT) has provided a new generation of business opportunities and commerce. Information has become a commodity and the networks that transfer and process it have become critical to the corporate and government infrastructure.

Every aspect of our society is influenced by the benefits of technology. However it is that same functionality that also hosts new threats, vulnerabilities and security implications. The concept of storing and processing information at incredible speeds and across vast distances without the need for human interaction has also generated an environment where the mysteries of technology can propagate a clouded perception that leads to a lack of trust and market confidence.

### **Requirement**

Greater and greater emphasis is being placed upon industry and commerce to demonstrate assurances of corporate governance, due diligence and a duty of care in relation to the manner in which information systems are protected and incidents and grievances resolved.

The European Convention on Human Rights, Articles 6 and 8, has emphasised a number of areas that impact on industry and commerce highlighting important implications in terms of the requirement to apply equitable protocols to disciplinary proceedings and expectations of privacy.

The principles of data protection are being applied in the vast majority of European countries and are especially enforced in the EU member states. Personal Data can only be processed for specific purposes and under controlled conditions. Data Protection legislation (in the UK it is set out in the Seventh Principle of the 1998 Act) highlights a requirement for appropriate technical and organisational measures to be taken to ensure that personal data is stored and processed in a secure manner. This process embraces the very ability to identify and respond to incidents that may represent a breach in that security.

No longer can accusatorial and detrimental comments be used to refer to an individual without them being substantiated by objective facts. In terms of computer related incidents those facts are contained as data held

on electronic media. Although evidence based on a computer is often compelling it is also extremely volatile in that the slightest process can destroy its integrity and therefore its value as evidence. The relevant information must be acquired in such a form that the integrity and continuity of the evidence is preserved in a forensically sound manner.

Driven by these requirements companies seek assurance that all incidents are being handled in a structured and fair manner. Where appropriate a professional forensic investigation is conducted that identifies and interprets the facts in an impartial and objective manner. Sweeping assumptions and voluntary solutions have been found to fail and ultimately be detrimental to the corporate objectives and public image.

At the outset it is never clear as to the true extent or impact suffered through the consequences of an incident. What appears, at first, to be a minor indiscretion subsequently transpires to be a serious incident with potentially catastrophic implications. All too often the decision to respond to an incident is deferred and deferred again in based on the mistaken assumption that it is a minor incident. It is only when the incident manifests itself again, and possibly again, that the true implications and impact are realised.

Based on this precept it is essential that a strategic approach be adopted for all incidents and that the rules of evidence be applied in every case as if it were a matter that would be prosecuted in the highest court demanding the highest evidential standards. Such evidence must satisfy a Judge and Jury that it is the same when presented to the court as it was when the accused had control of it. This process is often referred to as "continuity and integrity" or "chain of custody".

Internationally recognised standards are emerging not least of which is ISO 17799, promoting good practice for information security management. These standards clearly recognise the requirement and value in adopting a strategic and professional approach to incident handling. A dominant theme of ISO 17799 is the requirement for incident handling procedures and identifies the fact that the vast majority of organisations do not have, nor can afford, the requisite skills to address all aspects of information security.

In 1999 the Turnbull Committee conducted a study reflecting upon a number of previous recommendations addressing the need for company boards to consider all relevant risks including information security. There is no doubt that a fundamental element of these risks is the corporate strategy and ability to identify and respond to any circumstances that may transpire to be a breach of security.

Information and communication technology has enabled the conception of many new crimes, as well as new ways of committing old crimes. Commercial espionage as emerged as the one of the greatest concerns facing industry and commerce. Prior to the pervasion of desktop computing commercial information was inaccessible and resided in rows of filing cabinets. The advent of ICT has empowered the concept of

"information" and made it a commodity that can be accessed by anyone with the ability and transported across networks or in miniature removable media.

*"All information has a value it is just a question of how much and who to."*

Criminal analysts have identified the fact that traditional crimes are migrating towards new technology. Where fraud was committed on paper using a pen it is now committed on a computer using a keyboard. Statistics reveal that over 80% of computer crimes affecting companies are committed by, or with the assistance of, an inside agent. The vast majority of company fraud is discovered only by chance leading analysts to believe that the majority of crime in the workplace remains undetected. In addition to being the victims of such crime companies are finding their networks being used as the vehicles to create and deliver criminal acts. Inappropriate material, pornography and paedophilia, are frequently made, stored and distributed by employees during work hours and using company networks.

The general principal of criminal culpability is that we are all responsible for our conscious acts or omissions. This responsibility applies to corporate bodies as much as it does to an individual. A number of high-profile cases in recent years involving Internet Service Providers (ISPs) have supported and enforced this principle. Individuals acting on behalf of a corporate body who have consciously chosen not to respond to a particular situation and have been deemed, in law, to have allowed the continuation of the offence and therefore are guilty as the principal offender would be. This principle has serious implications in terms of paedophile or pornographic material. If the existence of such material is brought to the attention of a person, representing the management of the company, and a decision made to take no action then the culpability may extend to that person and the board of directors of the company.

These drivers, collectively or singularly, form the requirement placed upon any organisation or corporation to strategically address the manner in which incidents are handled, investigated and resolved. The corner stone to all of these requirements is a professional approach computer forensic investigations.

## **Value**

The concept of risk management has long been recognised as a valuable management process. Often combined with disaster recovery and business continuity plans, the processes of risk management ensure that a strategic approach is adopted to the development and maintenance of the security profile of a company. Although there are many methodologies adopted for a risk management process the majority tend to evolve around three key elements as follows:

- the assets to be protected
- the vulnerabilities of those assets

- the human threat against them.

Incidents are caused by a human being doing, or omitting to do, some act. A professional investigation will establish facts that tend to demonstrate who was responsible, the motivation, how it was achieved and what the real impact was. Tangible facts provide an invaluable foundation and analysis to identify and assess the true threat that is presented to an organisation. Substantiated facts create a firm foundation upon which a risk assessment and management process can be conducted. Tangible evidence of who did what, where, why and how provides objectivity in relation to the threat profile as well as an insight and test of the company's security posture.

Electronic commerce, e trading and business to business interaction rely entirely upon the harmonisation of trusted ICT infrastructure. Customers and business partners alike seek confidence in such interaction of networks. Through the process of interaction the corporate risk strategy must be shared. The implementation of a professional incident response adds a substantial value to the level of confidence offered to trading partners and customers by relieving any doubts that criminals have a greater capability than commercial security.

Consumer confidence is considered to be the single most important factor driving the growth of e-commerce. History has demonstrated the catastrophic effect of other systems, such as the financial markets, where confidence in the market has been lost. Studies carried out in the UK and analysis of events relating to computer crime has shown that public confidence has been threatened by a belief that industry lacks the ability to address computer related incidents. The assurance of a professional forensic investigation clearly dispels that misconception and demonstrates that all computer related incidents will be resolved impartially, legally and ethically.

Computer related incidents in the workplace frequently raise a number of management issues. One of the main issues is the risk of disaffecting a hitherto loyal employee by making an accusation or to risk the penalties and sanctions of failing to resolve a grievance. Without the knowledge of substantive facts management are compelled to adopt one position or another. A professional computer forensic investigation must be conducted objectively and independently. A timely and appropriate response will ensure that management are empowered to pursue an objective, and not subjective, course of action.

Computer crime has been analysed as three distinct elements that drive the potential threat and execution of such a crime. These elements, in simple terms, are:

- a) motivation to commit the crime
- b) the physical and technical ability to perform the act, and
- c) the perception that he will succeed.

A professional investigation and subsequent presentation of the facts (combined with expert analysis, conclusions and recommendations) will enable each of these elements to be identified and to some extent, measured. Correct analysis of these elements will enable each of them to be addressed, managed and controlled. The process of threat analysis has proved extremely valuable in prevention of crime and computer related incidents.

It is extremely unlikely that crime and related incidents will be eradicated from our society in the foreseeable future. The concept of a crime free society may well only occur in the pages of science fiction novels. The modern process of crime prevention focuses on the aim of designing out crime. The value of successful crime prevention has been recognised and quantified for many years.

## **Capability**

A professional computer forensic investigation must be one that offers assurances of independence, quality and standards. These can be best described in three distinct categories that, although may overlap and interact in certain aspects, represent the requisite core elements that are essential to a professional computer forensic investigation capability.

### Resources:

Specific resources are required that enable the preservation, integrity and security of computer based evidence. These resources include the following:

- hardware and media
- software applications
- physical resources
- human resources.

Hardware equipment and electronic storage media must comply with all International standards and guidelines for best practice. Such compliance must be documented and able to withstand the closest scrutiny.

Forensic software tools and utilities must be also comply with forensic standards as well as remain effective against ever evolving technology.

Resources must also include physical environment, fixtures and fittings that provide conditions that ensure the evidence is handled in accordance with the rules, ethics and regulations relating to integrity, continuity, confidentiality and security.

Human resources are also a strong consideration for a professional capability. An immediate response to a computer related incident can be essential to ensure that no evidence is lost, overlooked or contaminated.

Such a response may be demanded 24 hours a day /7 days a week/ 365 days a year.

## Skills

Individual skills are acquired through knowledge and understanding and are accumulated through a combination of professionally structured training and practical experience. The requisite skills will overlap and often duplicate themselves but in general terms there are four core skills essential to a professional capability. These core skills are as follows:

- technical knowledge
- investigative understanding and experience
- knowledge relating to the application of the law and protocols
- understanding and experience of high-tech crime trends and techniques.

Technical skills must include knowledge and experience relating to the use and administration of operating systems as well as all aspects of its vulnerabilities and security protocols. This knowledge needs to extend to all of the common operating platforms, internet protocols, business applications and programming languages.

Investigative skills must include the knowledge and understanding relating to the identification of sources of evidence, the means and knowledge on how to preserve, acquire, examine and analyse it. Additional experience is required to enable the professional and effective management of an investigation through knowledge of systems and application of experience.

Knowledge and understanding relating to the law, legal protocols, professional standards and regulations is critical to the identification and recognition of material that is relevant evidence. Evidence must be correctly and fairly acquired otherwise an investigation will be flawed and cannot substantiate its conclusions.

The ability to understand and recognise criminal trends and techniques in relation to high-tech crime is required to provide a focus for every investigation. Without such focus an investigation cannot be efficient or effective in working towards or achieving its objectives. An understanding of the motivation, ability and perceptions of the perpetrator, together with practical knowledge of the tools, techniques and trends commonly adopted, will ensure that, if properly applied, the objectives of an investigation will be met.

All of these skills must be present or available for a forensic capability to be considered as professional.

## Methodology

Resources and a skill-base on their own will not ensure that they are applied in a manner that ensures quality and evidential standards. The third, and most important, element is that of adherence to a professional methodology. It must be capable of recognising all of the requirements and needs for a professional computer forensic investigation. Such a methodology must establish a benchmark standard and describe appropriate procedures and management systems that will deliver substantive facts that achieve the objective of the investigation.

## **Development**

### In-House

The development and maintenance of an in-house computer forensic capability offers itself as an attractive solution. The first barrier always appears to be the acknowledgement of the requirement to investigate such incidents followed by the allocation of funds and budgeting. Although this paper does not seek to estimate the costs and analyse the benefits there are a number of factors that should be considered.

The availability of an in-house team can be managed and tailored to meet the demand of the organisation. When not utilised human resources can be re-deployed to more effective duties. Demands for unsocial or extended hours can be addressed through internal management and deployment of staff. The control of sensitive and confidential information can be managed with closer scrutiny. Breaches of confidentiality can be dealt with discreetly and summarily.

However skills that are not used or refreshed with wider experiences will degrade and become stale and ineffective. The field of computer forensic investigation has to evolve in step and pace with technology. New forensic resources and revised investigation techniques are constantly emerging. By comparison to any other profession, such as lawyers or accountants, it is evident that advice and guidance must be accurate, correct and current.

### Out-Source

An out-sourced computer forensic capability must be able to demonstrate that it possesses and maintains the appropriate resources, skills and methodology. It must be capable of offering quality assurance and an approach that is entirely independent based on professional ethics and integrity. For the purpose of computer forensic investigations a professional approach is seen as one that is objective and able to deliver an accurate result based on integrity, as opposed to one that simply tells a customer what they want to hear.

A professional service will, in the long-term, offer substantial cost benefits through the delivery of results that are independent, objective and will stand up to judicial scrutiny. A professional out-sourced capability will

have to share the business risk associated with a flawed or failed investigation.

An external or out-sourced capability must maintain its professional status through constant investment in the research and development of skills and resources as well as the evolution of expert methodologies. This investment in intellectual capital must be evident in out-sourced service providers but harder to justify with in-house teams.

## **Conclusion**

The requirement for a professional approach to the investigation of computer related incidents are clear and present. It will continue to be driven forward by social and commercial requirements and expectations. International standards are emerging from many corners of the globe placing greater emphasis on human rights and equity in the workplace. The bespoke forensic resources that are available are few and often conflict with each other as a result of product competition.

The requisite expert skills are diverse and require a procedure along which they can be applied. This application requires a team approach and corresponding investment in intellectual capital is only possible through a dedicated resource specialising in professional computer forensic services.

The conclusion of this paper is that the vast majority of industry and commerce will, in the medium-term, require some level of computer forensic service whether to assist with adopting strategies and policies or to respond to an incident. Those few specific sectors who will choose to develop an in-house solution may well seek consultancy advice and expert support as investigations become too complex or too voluminous.

It is the conclusion of this paper that the companies who will lead the world market in the provision of computer forensic investigation services will be those who develop and maintain an expert skill base and demonstrate professional standards of quality, integrity and efficiency.