

# AN INTRODUCTION TO FORENSIC READINESS PLANNING

## TECHNICAL NOTE 01/2005

**27 MAY 2005**

This paper was previously published by the National Infrastructure Security Co-ordination Centre (NISCC) – a predecessor organisation to the Centre for the Protection of National Infrastructure (CPNI).

Hyperlinks in this document may refer to resources that no longer exist. Please see CPNI's website ([www.cpni.gov.uk](http://www.cpni.gov.uk)) for up-to-date information.

### **Disclaimer**

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

## Key Points

- A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security incident or computer-related crime. In fact there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs.
- Forensic readiness is introduced as the ability of an organization to maximise its potential to use digital evidence whilst minimizing the costs of an investigation.
- Forensic readiness addresses a number of key business risks by providing evidence to detect and deter crime such as fraud, information theft, internet abuse, and by preparing an organisation for the use of digital evidence in its own defence.
- Preparing to use digital evidence may involve enhanced system and staff monitoring; technical, physical and procedural means to secure data to evidential standards of admissibility; processes and procedures to ensure that staff recognize the importance and legal sensitivities of evidence; obtaining appropriate legal advice and interfacing with law enforcement.
- This paper outlines a ten step approach to forensic readiness planning.

## Overview

This paper is intended for those with responsibility for, or potential involvement in, computer investigations. An investigation using evidence residing on an organization's IT systems is likely to involve a wide variety of staff, from information security officers to general security personnel, from human resource managers to the chief information officer. To proceed successfully, a coherent and managed process should be in place where all internal roles and responsibilities are clear and any necessary external relationships are established. Preparation for a Digital Forensic Investigation (DFI) is known as forensic readiness. The aim of this document is to present the outline of a forensic readiness planning process that an organization can adopt and adapt to its specific requirements.

## Introduction

Forensic readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.

A DFI is commonly employed on a serious information security or criminal incident. The typical case is when the PC of a suspect has been seized, the hard-drive is imaged and an investigation proceeds to search for traces of evidence. The examination is conducted in a systematic, standardised and legal manner to ensure the admissibility of the evidence. It is essentially a post-event recovery of digital evidence.

In a business context there is the opportunity to actively collect potential evidence in the form of logfiles, emails, back-up disks, portable computers, network traffic records, and telephone records, amongst others. This evidence may be collected in advance of a crime or dispute, and may be used to the benefit of the collecting organisation if it becomes involved in a formal dispute or legal process.

Recourse to litigation is generally a last resort for most organisations, so why be concerned about potential evidence and related disputes? Digital evidence can help manage the impact of some important business risks. Digital evidence can support a legal defence; it could support a claim to IPR; it could show that due care (or due diligence) was taken in a particular process; it could verify the terms of a commercial transaction; and it could lend support to internal disciplinary actions. To succeed in a legal process it is therefore essential that the organisation has actively gathered the evidence it is likely to require. Moreover, it is vital to have the capability to process evidence cost effectively, and to have suitably trained staff who know how to ensure potential digital evidence is preserved. An organisation also needs to be able to take appropriate and informed decisions in the light of the business risk. Therefore, it is necessary from the outset to consider the importance of evidence and to be prepared to gather it for a wide range of scenarios, for example:

- threats and extortion;
- information compromise;
- accidents and negligence;
- stalking and harassment;
- commercial disputes;
- disagreements, deceptions and malpractice;
- property rights infringement;
- economic crime e.g. fraud, money laundering;
- content abuse;
- privacy invasion and identity theft; and
- employee disciplinary issues.

Being prepared to gather and use evidence can also have benefit as a deterrent. A good deal of crime is internal. Staff will know what the organisation's attitude is towards the policing of corporate systems. They will know, or will hear rumours, as to what type of crimes may have been successfully or unsuccessfully committed and what action may have been taken against staff. A company showing that it has the ability to catch and prosecute this type of insider attacker will dissuade them, much like the shop sign 'We always prosecute thieves'.

## **Forensic Readiness**

Digital evidence is required whenever it can be used to support a formal process. An organisation therefore requires access to the evidence that will be able to support its position in such an event. Thus there is a business requirement for digital evidence to be available even before an incident occurs.

In a forensic readiness approach, this incident preparedness becomes a corporate goal and consists of those actions, technical and non-technical, that maximise an organisation's ability to use digital evidence. Any computer data may become used in a formal process and may need to be subject to forensic practices. The ability of an organisation to exploit this data is the focus of forensic readiness. Forensic readiness is incident anticipation for incident response. Its purpose is to support the business requirement to use digital evidence.

From the discussion above and the objectives of forensic readiness we can see that good forensic readiness can offer an organisation the following benefits:

- evidence can be gathered to act in an organisation's defence if subject to a lawsuit;
- comprehensive evidence gathering can be used as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cyber-criminal);
- in the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal disruption to the business;
- a systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- a structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);
- forensic readiness can extend the scope of information security to the wider threat from cyber crime, such as intellectual property protection, fraud, extortion etc;
- it demonstrates due diligence and good corporate governance of the company's information assets;
- it can demonstrate that regulatory requirements have been met;
- it can improve and facilitate the interface to law enforcement if involved;

- it can improve the prospects for a successful legal action;
- it can provide evidence to resolve a commercial dispute; and
- it can support employee sanctions based on digital evidence (for example to prove violation of an acceptable use policy).

## **10 Steps for Forensic Readiness Planning**

In order to plan for a digital investigation we first need to understand the goals of forensic readiness:

- to gather admissible evidence legally and without interfering with business processes;
- to gather evidence targeting the potential crimes and disputes that may adversely impact an organisation;
- to allow an investigation to proceed at a cost in proportion to the incident;
- to minimise interruption to the business from any investigation; and
- to ensure that evidence makes a positive impact on the outcome of any legal action.

The following ten steps describe the key activities in forensic readiness planning:

1. define the business scenarios that require digital evidence;
2. identify available sources and different types of potential evidence;
3. determine the evidence collection requirement;
4. establish a capability for securely gathering legally admissible evidence to meet the requirement;
5. establish a policy for secure storage and handling of potential evidence;
6. ensure monitoring is targeted to detect and deter major incidents;
7. specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
8. train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence;
9. document an evidence-based case describing the incident and its impact; and
10. ensure legal review to facilitate action in response to the incident.

The remainder of this paper gives a brief description of each of the ten steps.

### **1. Define the business scenarios that require digital evidence**

The first step in forensic readiness is to define the purpose of an evidence collection capability. The rationale is to look at the risk and potential impact on the business from the various types of crimes and disputes. What is the threat to the business and what parts are vulnerable? This is, in effect, a risk assessment, and is performed at the business level. The aim is to understand the business scenarios where digital evidence may be required and may benefit the organisation the event that it is required. In general the areas where digital evidence can be applied include:

- reducing the impact from computer-related crime;
- dealing effectively with court orders to release data;
- demonstrating compliance with regulatory or legal constraints;
- producing evidence to support company disciplinary issues;
- supporting contractual and commercial agreements; and
- proving the impact of a crime or dispute.

In assessing these scenarios, this step provides an indication of the likely benefits of being able to use digital evidence. If the identified risks, and the potential benefits of forensic readiness, suggest a good return on investment is achievable, then an organisation needs to consider what evidence to gather for the various risk scenarios.

## **2. Identify available sources and different types of potential evidence**

The second step in forensic readiness is for an organisation to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. Computer logs can originate from many sources. The purpose of this step is to scope what evidence may be available from across the range of systems and applications in use.

Some basic questions need to be asked about possible evidence sources to include.

- Where is data generated?
- What format is it in?
- How long is it stored for?
- How is it currently controlled, secured and managed?
- Who has access to the data?
- How much is produced?
- Is it archived? If so where and for how long?
- How much is reviewed?
- What additional evidence sources could be enabled?
- Who is responsible for this data?
- Who is the formal owner of the data?
- How could it be made available to an investigation?
- What business processes does it relate to?
- Does it contain personal information?

Email is an obvious example of a potential rich source of evidence that needs careful consideration in terms of storage, archiving and auditing and retrieval. But this is not the only means of communication used over the internet, there is also instant messaging, web-based email that bypasses corporate email servers, chat-rooms and newsgroups, even voice over the internet. Each of these may need preserving and archiving.

The range of possible evidence sources includes:

- equipment such as routers, firewalls, servers, clients, portables, embedded devices etc;
- application software such as accounting packages etc for evidence of fraud, erp packages for employee records and activities (e.g. in case of identity theft), system and management files etc;
- monitoring software such as intrusion detection software, packet sniffers, keyboard loggers, content checkers, etc;
- general logs such as access logs, printer logs, web traffic, internal network logs, internet traffic, database transactions, commercial transactions etc;
- other sources such as: cctv, door access records, phone logs, pabx data etc; and
- back-ups and archives.

### **3. Determine the Evidence Collection Requirement**

It is now possible to decide which of the possible evidence sources identified in step 2 can help deal with the crimes and disputes identified in step 1 and whether further ways to gather evidence are required. This is the evidence collection requirement.

The purpose of this step is to produce an evidence requirement statement so that those responsible for managing the business risk can communicate with those running and monitoring information systems through an agreed requirement for evidence.

One of the key benefits of this step is the bringing together of IT with the needs of corporate security. IT audit logs have been traditionally configured by systems administrators independently of corporate policy and where such a policy exists there is often a significant gap between organisational security objectives and the 'bottom-up' auditing actually implemented.

The evidence collection requirement is moderated by a cost benefit analysis of how much the required evidence will cost to collect and what benefit it provides (see above). The critical question for successful forensic readiness is what can be performed cost effectively. By considering these issues in advance and choosing storage options, auditing tools, investigation tools, and appropriate procedures it is possible for an organisation to reduce the costs of future forensic investigations.

### **4. Establish a capability for securely gathering legally admissible evidence to meet the requirement**

At this point the organisation knows the totality of evidence available and has decided which of it can be collected to address the company risks and within a planned budget. With the evidence requirement understood, the next step is to ensure that it is collected from the relevant sources and that it is preserved as an authentic record.

At this stage legal advice is required to ensure that the evidence can be gathered legally and the evidence requirement can be met in the manner planned. For example, does it involve monitoring personal emails, the use of personal data, or 'fishing trips'<sup>1</sup> on employee activities? In some countries, some or all of these activities may be illegal. Relevant laws, in the areas of data protection, privacy and human rights, will inevitably constrain what can actually be gathered.

In the UK the information commissioner has stated:

- monitoring should be targeted at specific problems;
- it should only be gathered for defined purposes and nothing more; and
- staff should be told what monitoring is happening except in exceptional circumstances.

Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage. As well as preventative measures such as secure rooms and swipe card access it is also prudent to have records of who has access to the general location and who has access to the actual machines containing evidence. Any evidence or paperwork associated with a specific investigation should be given added security by, for example, storing in a safe. Additional security of logs can also be achieved through the use of WORM storage media.

## **5. Establish a policy for secure storage and handling of potential evidence**

The objective of this step is to secure the evidence for the longer term once it has been collected and to facilitate its retrieval if required. It concerns the long-term or off-line storage of information that might be required for evidence at a later date.

A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence. In the parlance of investigators this is known as continuity of evidence (in the UK) and chain of custody (in the US). The continuity of evidence also includes records of who held, and who had access to, the evidence (for example from swipe control door logs).

A significant contribution to the legal collection of evidence is given by the code of practice on the legal admissibility and weight of information stored electronically, published by the British Standards Institution. This document originated from a perceived need for evidence collection in the paperless office. The problem it addressed is if all paper documents are scanned, can the paper sources be thrown away without loss of evidential usability? The current edition broadens the scope to all information management systems

---

<sup>1</sup> Ad hoc opportunistic searches, without justification, for potentially incriminating activities or communication.

such as those where information is transmitted over networks such as email systems for example. It points out that methods of storage, hardware reliability, operation and access control, and even the programs and source code, may be investigated in order to determine admissibility. A closely related international standard is being developed as ISO 15801.

The required output of this step is a secure evidence policy. It should document the security measures, the legal advice and the procedural measures used to ensure the evidence requirement is met. Upon this document rests the likely admissibility and weight of any evidence gathered.

## **6. Ensure monitoring and auditing is targeted to detect and deter major incidents**

In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatened incidents in a timely manner. This is directly analogous to Intrusion Detection Systems (IDS), extended beyond network attack to a wide range of behaviours that may have implications for the organisation. It is all very well collecting the evidence. This step is about making sure it can be used in the process of detection. By monitoring sources of evidence we can look for the triggers that mean something suspicious may be happening.

The critical question in this step is when should an organisation be suspicious? A suspicious event has to be related to business risk and not couched in technical terms. Thus the onus is on managers to explain to those monitoring the data what they want to prevent and thus the sort of behaviour that IDS might be used to detect for example. This should be captured in a 'suspicion' policy that helps the various monitoring and auditing staff understand what triggers should provoke suspicion, who to report the suspicion to, whether heightened monitoring is required, and whether any additional security measures should be taken as a precaution.

Each type of monitoring should produce a proportion of false positives. The sensitivity of triggers can be varied as long as the overall false positive rate does not become so high that suspicious events cannot be properly reviewed. Varying triggers also guards against the risk from someone who knows what the threshold on a particular event is and makes sure any events or transactions he wishes to hide are beneath it.

## **7. Specify circumstances when escalation to a full formal investigation (which may use digital evidence) is required**

Some suspicious events can be system generated, such as by the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness. Each suspicious event found in step 6 needs to be reviewed. Either an event will require escalation if it is clearly serious enough, or it will require enhanced monitoring or other precautionary measures, or it is a false positive. The purpose of this step is to decide how to react to the suspicious event.

The decision as to whether to escalate the situation to management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed. The decision criteria should be captured in an escalation policy that makes it clear when a suspicious event becomes a confirmed incident. At this point an investigation should be launched and policy should indicate who the points of contact are (potentially available on a 24x7 basis) and who else needs to be involved.

As with steps 3 and 6, the network and IT security managers and the non-IT managers need to understand each other's position. What level of certainty or level of risk is appropriate for an escalation? What strength of case is required to proceed? A preliminary business impact assessment should be made based on whether any of the following are present:

- evidence of a reportable crime;
- evidence of internal fraud, theft, other loss;
- estimate of possible damages (a threshold may induce an escalation trigger);
- potential for embarrassment, reputation loss;
- any immediate impact on customers, partners or profitability;
- recovery plans have been enacted or are required; and
- the incident is reportable under a compliance regime.

## **8. Train staff, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence**

A wide range of staff may become involved in a computer security incident. The aim of this step is to ensure that appropriate training is developed to prepare staff for the various roles they may play before, during and after an incident. It is also necessary to ensure that staff are competent to perform any roles related to the handling and preservation of evidence.

There will be some issues relevant to all staff if they become involved in an incident. The following groups will require more specialised awareness training for example:

- the investigating team;
- corporate HR department;
- corporate PR department (to manage any public information about the incident);
- 'owners' of business processes or data;
- line management, profit centre managers;
- corporate security;
- system administrators;
- IT management;
- legal advisers; and

- senior management (potentially up to board level).

At all times those involved should act according to 'need to know' principles. They should be particularly aware whether any staff, such as 'whistle blowers' and investigators, need to be protected from possible retaliation by keeping their names and their involvement confidential. Training may also be required to understand the relationships and necessary communications with external organisations that may become involved

## **9. Present an evidence-based case describing the incident and its impact**

The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. The questions go along the lines of who, what, why, when, where and how. Credibility is provided by evidence and a logical argument. The purpose of this step is to produce a policy that describes how an evidence-based case should be assembled. A case file may be required for a number of reasons:

- to provide a basis for interaction with legal advisers and law enforcement;
- to support a report to a regulatory body;
- to support an insurance claim;
- to justify disciplinary action;
- to provide feedback on how such an incident can be avoided in future;
- to provide a record in case of a similar event in the future (supports the corporate memory so that even if there are changes in personnel it will still be possible to understand what has happened); and
- to provide further evidence if required in the future, for example if no action is deemed necessary at this point but further developments occur.

## **10. Ensure legal review to facilitate action in response to the incident**

At certain points during the collating of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions. Legal advisers should be able to advise on the strength of the case and suggest whether additional measures should be taken; for example, if the evidence is weak is it necessary to catch an internal suspect red handed by monitoring their activity and seizing their PC?

Any progression to a formal action will need to be justified, cost-effective and assessed as likely to end in the company's favour. Although the actual decision of how to proceed will clearly be post-incident, considerable legal preparation is required in readiness.

Legal advisors should be trained and experienced in the appropriate cyber-laws and evidence admissibility issues. They need to be prepared to act on an incident, pursuant to the digital evidence that has been gathered and the case

presented in step 9. Legal advice should also recognise that the legal issues may span legal jurisdictions e.g. states in the US, member states in the EU. Advice from legal advisers will include:

- any liabilities from the incident and how they can be managed;
- finding and prosecuting/punishing (internal versus external culprits);
- legal and regulatory constraints on what action can be taken;
- reputation protection and PR issues;
- when/if to advise partners, customers and investors;
- how to deal with employees;
- resolving commercial disputes; and
- any additional measures required.

## **Concluding Remarks**

Forensic readiness is an organisation's ability to use digital evidence when required. Its aim is to maximise an organisation's ability to gather and use digital evidence whilst minimising the costs of related investigations. The proposed ten steps to forensic readiness lay out a practical approach to the policies and practices required for an organisation to achieve a forensic readiness capability.

Forensic readiness is complementary to, and an enhancement of, many existing information security activities. It should be part of an information security risk assessment to determine the possible disputes and crimes that may give rise to a need for electronic evidence. It is closely related to incident response and business continuity, to ensure that evidence found in an investigation is preserved and the continuity of evidence maintained. It is part of security monitoring, to detect or deter disputes that have a potentially major business impact. Forensic readiness also needs to be incorporated into security training.

Many organisations will already perform some of the activities required to effectively collect and exploit electronic evidence in place as part of their general information security, incident response and crime prevention activities. What is needed in most organisations is a systematic and proactive approach to the gathering and preserving of evidence to meet their business needs. In practice, forensic readiness policies may be achieved through incremental enhancement to existing policies such as data retention, incident response, information security, crime prevention etc.

A cautionary tale serves to illustrate the state of forensic readiness in one organisation. An investigator reported an occasion when he was asked to look into investigating an employee suspected of stealing software, customer databases and marketing and business plans. The employee had been on 'gardening' leave for six weeks without any evidence to support the company suspicions. Unfortunately a litany of errors had virtually eliminated the chance of finding any incriminating evidence. The suspect had been allowed to keep his laptop, PDA and mobile phone. His desktop PC had been re-formatted, a

new operating system installed and had been given to another employee. Remote access accounts had been kept active. His desk had been cleared. His files on the fileserver had been removed and mails on the mail-server had been deleted en masse. Back-up tapes potentially containing useful files had been re-cycled. Email was un-retrievable. The organisation had no evidence with which to support any allegations against the employee.

Forensic readiness would allow an organisation to avoid these mistakes.

## About the Author

Dr Rowlingson is a principal consultant in information security at QinetiQ ([www.qinetiq.com](http://www.qinetiq.com)), formerly the Defence Evaluation and Research Agency (DERA). His current research interests include digital evidence and computer-related crime, security in open source software and the security of home computer users. He managed QinetiQ's participation in the European CTOSE project on digital evidence ([www.ctose.org](http://www.ctose.org)) and continues to work with the CTOSE Foundation. He is also widely experienced in developing research strategy. In a previous incarnation he was a member of the DERA team which developed the Architecture Neutral Distribution Format (ANDF) for the Open Software Foundation.