A Ten Step Process for Forensic Readiness

Robert Rowlingson Ph.D
QinetiQ Ltd.

Abstract

A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security incident. In fact, there are many circumstances where an organisation may benefit from an ability to gather and preserve digital evidence before an incident occurs. Forensic readiness is defined as the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation. The costs and benefits of such an approach are outlined. Preparation 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 recognise the importance and legal sensitivities of evidence, and appropriate legal advice and interfacing with law enforcement. This paper proposes a ten step process for an organisation to implement forensic readiness.

Introduction

Digital forensic investigations (DFIs) are commonly employed as a post-event response to a serious information security or criminal incident. They typically consider the case 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, formalised and legal manner to ensure the admissibility of the evidence. The process of a digital forensic investigation is subject to considerable scrutiny of both the integrity of the evidence [Sommer 1998], and the integrity of the investigation process [Stephenson 2002, 2003b].

This scenario of a DFI, and most discussions of the forensic process, tend to ignore what happens to the object of the investigation prior to the decision to undertake an investigation. The necessary evidence either exists, and hopefully is found by the DFI, or it does not exist and a suspect cannot be charged and prosecuted. This is the law enforcement view of a DFI. It begins when a crime has been committed or discovered and investigators attend a crime scene or wish to seize evidence [ACPO 2003, ENFSI 2003]. The quality and availability of evidence is a passive aspect of the DFI.

In a business context however, 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 can be used to the benefit of the collecting organisation.

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

Being prepared 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 toward 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."

Information security programmes often focus on prevention and detection measures. From a preventative information security perspective there is little need for digital evidence. From a business perspective, however, there are a number of scenarios where collecting appropriate digital evidence would be beneficial. Thus, there is a business requirement for digital evidence to be available even before an incident occurs. What exactly this requirement is, how it is met, and how organisations can exploit digital evidence has not previously been considered in detail.

Forensic Readiness

The business requirement to gather and use digital evidence has been recognized in a number of recent papers. Yasinsac and Manzano (2002) note that enterprise policies can enhance computer and network forensics. They propose six categories of policies to facilitate DFI. Their categories are designed to help enterprises deter computer crime and position themselves to respond to successful attacks by improving their ability to conduct DFI:

- Retaining Information;
- Planning the Response;
- Training;
- Accelerating the Investigation;
- Preventing Anonymous Activities;
- Protecting the Evidence.

Wolfe-Wilson and Wolfe (2003) discuss management strategies for implementing forensic security measures. They stress the need for an organisation to be in control of

a DFI and to have planned procedures in place to preserve digital evidence and to instigate a forensic investigation. They note important links with the Business Continuity Plan and Incident Response procedures. The paper also notes the role of forensics within an overall security policy and strategy.

Carrier and Spafford (2003) present an investigation process model which, whilst focusing on the investigation itself, also recognises a readiness phase to ensure that the operations and infrastructure are able to fully support an investigation.

Tan (2002) introduced the concept of forensic readiness to cover two objectives:

- Maximising an environment's ability to collect credible digital evidence;
- Minimising the cost of forensics during an incident response.

The problem was approached from the need to reduce the time and costs of a forensic examination. Tan quotes the example of the HoneyNet project forensic challenge (http://www.honeynet.org/challenge/results/index.html) where half an hour of attacker time required an average investigation time of 48 hours. Tan also discussed technical aspects such as time-stamping, system hardening and compromised kernels, and noted five factors that affect evidence preservation and investigation time:

- How logging is done;
- What is logged;
- Intrusion detection systems;
- Forensic acquisition;
- Evidence handling.

The message from Yasinsac and Manzano (2002) and Wolfe-Wilson and Wolfe (2003) suggests there is a broad organisational role in the forensic readiness process. Tan, in effect, presents the idea of system forensic readiness as one part of overall enterprise forensic readiness. Viewed from an enterprise perspective, forensic readiness can be seen as the ability of an organisation to maximise its potential to use digital evidence when required.

Digital evidence is required whenever it can be used to support a legal process. An organisation, therefore, requires access to the evidence that will be able to support its position in such an event. This is not as easy as it might seem; relevant evidence is unlikely to exist by default. In any computer security incident there will be a tendency to focus on containment and recovery, as these are the foremost business critical issues. However, in stressing these, any evidence that might be required may be damaged, discarded or simply ignored [Tan et al 2003]. There is a trade-off to be made between recovery and evidence. A lot of information is also lost or discarded as part of normal business practice. 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 evidence is preserved. The organisation also

needs to be able to make appropriate and informed decisions in the light of the business risk.

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.
In this paper, a number of issues are introduced which help take this concept further:

1) Within organisations there is concern with a wide range of crimes and disputes, such as fraud and theft, that may be addressed with digital evidence - not just information security defence against criminal hackers;
2) An organisation can be involved with all aspects of an investigation - not just the digital forensics;
3) An organisation will assess the costs of additional measures to prepare for DFIs compared with the potential benefits; in general, investigations should be cost-effective not just technically feasible;
4) In a corporate environment there is a wide range of potential evidence sources; digital evidence must be actively sought, not passively used;
5) In a corporate environment, staff configuring audit logs may not be aware of the "high-level" crimes and business issues that logging could be used to detect;
6) To collect useful evidence an organisation needs to target its collection capability on the risks to the business; it is not a technical issue of what should be recorded in logfiles;
7) Monitoring to detect an incident can encompass a wide range of techniques including CCTV, door swipes, and honeypots. It is not just a case of applying an intrusion detection system;
8) To collect admissible evidence, the organisation needs to review the legality of any monitoring; it is not a technical issue of what can be 'sniffed' or traced;
9) The requirement for evidence implies that all forms of potential evidence should be considered, such as CCTV cameras, personnel records, access control systems etc. - not just logfiles and hard disks;
10) A wide range of staff may become involved in an investigation and will need to understand their roles within it; it is not just a job for the forensic investigator or system managers;
11) When an incident occurs, the appropriate response must consider the options for forensic investigation and evidence preservation, not just the immediate business continuity needs of containment, eradication and recovery;
12) A major criminal incident may involve the police. Prior discussions with them can facilitate the interaction when an incident occurs;
13) A major incident may become public knowledge and have reputation and share-price ramifications, so company lawyers and media managers may be involved. It is not just an internal departmental issue;
14) The preservation of digital evidence may be required for corporate governance or regulatory enforcement; it is not just an internal company issue

In the context of enterprise security the definition of forensic readiness can be broadened to:

> *the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.*

Excluded from this definition are preventative and recovery measures. It is assumed that appropriate information security defences, such as system hardening, are implemented and revised as part of any security incident. Similarly, it is assumed that a competent Computer Security Incident Response Team (CSIRT) is available [Schultz and Shumway 2002]. Forensic readiness is incident anticipation compared with incident response. Forensic readiness concerns itself with enabling the business requirement to use digital evidence. Information security, in general, concerns itself with ensuring that the business utility of information systems is maintained, and this includes ensuring the business requirement for digital evidence is met.

The Costs and Benefits of Forensic Readiness

If forensic readiness is an enterprise issue, then the extent to which it can be pursued will depend on the organisation obtaining value for money for any investment. The foremost issue in understanding the need for forensic readiness is a risk assessment. An extant risk assessment for something like BS 7799 or ISO17799 will be a valid starting point, but may not assess all the situations where digital evidence may be required. An asset register is certainly needed with an indication of the attractiveness of targets to the various types of crime such as fraud, malicious damage, and IPR theft, as well as an understanding of the impact on the company should such an event take place.

Any information security defensive measures based on a risk assessment will always leave a residual risk. Often this is because users are trusted not to cause a security incident. In the long run, such an assessment may be correct and stringent defensive measures may not be required. In forensic readiness, however, it is necessary to assume that an incident will occur, even if a risk assessment says it should not. This is especially true of situations where the risk is highest from insiders. It may be infeasible to deploy preventative measures, especially where staff have to be trusted with high value assets, but effective deterrence may be achieved with forensic readiness. Depending on the impact of such an event, an organisation may need to put in place measures to identify any miscreant and obtain the evidence required to take appropriate action against them. Once an organisation recognises that it requires some form of investigative capability, the next step is to ensure the efficiency and competency of that capability.

From the discussion above and the objectives of forensic readiness it is evident that good forensic readiness can offer an organisation the following benefits:

- Evidence can be gathered to act in the company'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 target of information security to the wider threat from cyber crime, such as intellectual property protection, fraud, or extortion;
- 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;
- It can support employee sanctions based on digital evidence (for example, proving violation of an acceptable use policy).

The costs of implementing forensic readiness may be significant, particularly in an organisation with immature information security management processes. However, the costs are significantly ameliorated if the organisation has already performed a comprehensive risk assessment, implemented a business continuity plan, and has programmed information security into staff training. In a more security-aware organisation, forensic readiness can add value to many existing processes and leverage such activities as incident response, business continuity, and crime prevention. In any event, the issues raised by the need for forensic readiness need to be brought to senior management or board attention. Arguably a decision at this level should authorise an enterprise forensic readiness programme.

The sorts of activities where costs will be incurred include:

- Updates to policies;
- Improvements in training;
- Systematic gathering of potential evidence;
- Secure storage of potential evidence;
- Preparation for incidents;
- Enhanced capability for evidence retrieval;
- Legal advice;
- Developing an in-house DFI capability, if required.

Technical measures and appropriate products may also be required, for example to facilitate archiving and retrieval of data or to improve monitoring and logging, but in general, forensic readiness is a security process which is more procedural and staff-intensive than technological.

Although it is likely that certain new procedures and policies will be necessary to implement forensic readiness, it should not entail a whole new set of procedures. In practice, forensic readiness policies may be achieved through incremental enhancement to existing policies, such as data retention, incident response, information security, and crime prevention. This will allow much more value to be extracted from them, by targeting specific incidents and crimes that might otherwise have not received a high priority.

Dealing with Incidents and Evidence

The typical picture of a DFI involves targeting computer media, principally a PC hard drive, to recover admissible digital evidence. However, a corporate incident and the subsequent need for evidence may go much further. Melia (2002) states "it is critical for investigators to understand the distinction between examining such local media and conducting a full-scale computer-incident forensic investigation." This reference principally focuses on computer fraud investigation, but the principle extends to a wide range of incidents that can impact an organisation, for example:

- Threats and extortion;
- Accidents and negligence;
- Stalking and harassment;
- Commercial disputes;
- Disagreements, deceptions, and malpractice;
- Property rights infringement;
- Economic crime e.g. fraud, money laundering;
- Content abuse;
- Privacy invasion and identity theft;
- Employee disciplinary issues.

This range of disputes is reflected in the range of staff who are potentially involved with an incident. Forensic readiness actually applies all through the company, as a wide range of staff will be involved with, impacted by, or responsible for, evidence and investigations; for example:

- The investigating team;
- The investigation subjects (i.e. suspects);
- Corporate HR department;
- Corporate PR department;
- "Owners" of business processes or data;
- Line management, Profit centre managers;

- Claimant (e.g. dismissed employee, organisation in dispute, or customer claiming infringement of Data Protection Act);
- Staff (e.g. colleagues of people under investigation);
- Corporate security;
- IT staff;
- Legal advisers.

There are also potential dependencies and interactions with external organisations:

- Police (not necessarily local force, especially if defending against allegations from overseas, or if the organisation is multi-national);
- Other law enforcement authority (e.g. HM Customs and Excise, Trading Standards or Serious Fraud Office);
- Overseas prosecution authority or court;
- Trade Union / Staff Association representatives;
- Internal or external auditors;
- Regulatory authorities (e.g. Financial Services Authority, Data Protection Commissioner, Bank of England);
- Customers, suppliers, partner organisations;
- Facilities management organisations (e.g. companies to whom IT or building security has been out-sourced);
- The media – due to the need to manage the PR impact of any incident.

Therefore, forensic readiness requires and enables a corporate approach to digital evidence. Organisations need staff trained in the sensitivities of evidence, in company investigation policy, and the external interface. Implementing forensic readiness requires an understanding of the possible evidence sources, how to gather evidence legally and cost-effectively, when to escalate a suspicious event into a formal forensic investigation, and how to put together a case with the possible involvement of law enforcement agencies.

A further conflict can arise when it comes to incident response. Post-incident containment, eradication, and recovery (CER) activities are focused on as the most important business issues. However, a rapid recovery exercise may overlook or delete data that could be useful in identifying the causes (and culprits) of incidents. On the other hand, retrieving evidence and handling an investigation in a forensic manner may impose cost and time delays on incident recovery. A digital investigation must therefore be seen as a trade-off between evidence preservation, and CER. Good forensic readiness can allow the impact on CER to be minimised. Forensic readiness can be tested as part of business continuity and disaster recovery exercises

10 Steps to Forensic Readiness

For enterprise forensic readiness to progress, the above discussion must be presented in a way that will facilitate a practical implementation for organisations. Firstly, proposed the goals of forensic readiness are as follows:

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

The following ten steps describe the key activities in implementing a forensic readiness programme.

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

The assumption is made that appropriate defensive (preventative) security measures are in place in accordance with a risk assessment and that the risk assessment has sufficient information to understand the risks to the organisation from incidents where digital evidence may be required.

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 in terms of:

- Reducing the impact of computer-related crime.

Organisations are at risk from a wide variety of computer-related crime. The risks from computer-related crime should be assessed using any extant assessments of risks to crime. Further analysis can consider the various classes of threats to information systems [Jones and Sutherland 2003]. A threat assessment is an assessment of the potential for a crime to be committed. Crime by insiders also needs to be carefully assessed [Schultz and Shumway 2002]. Issues to consider include: Where are people trusted? Where is the money? Where are critical points of failure? A vulnerability assessment is also required, not in terms of IT vulnerabilities, but process vulnerabilities and the attractiveness of targets to criminals.

- Dealing effectively with court orders to release data.

Depending on the business of the organisation the types of evidence likely to be required by a court may vary. Some will be common to all organisations, such as email. The likelihood of such evidence being required should also be assessed: Is it a particularly litigious business sector? Are there any particularly sensitive or controversial activities that might lead to a court case?

- Demonstrating compliance with regulatory or legal constraints.

This requirement can be business-specific, for example the Basel2 regulations for banks, but with the introduction of laws governing issues, such as electronic document retention [Patzakis 2002], it is becoming increasingly important. A further example might be to provide evidence of controls and company communications that show due care in circumstances that have the potential for negligence claims.

A key legal requirement in most jurisdictions is that potential evidence must not be destroyed. The duty to preserve evidence may arise when litigation is filed or can be reasonably anticipated. Spoliation may be a criminal offence, so an ability to implement a particular evidence preservation process at short notice (which may not be required at other times) could be valuable.

- Producing evidence to support company disciplinary issues.

Typically, this may be showing contravention of the company internet acceptable use policy, but there are many other issues where an organisation could use digital evidence, such as door swipe logs and phone logs, to support a case in a disciplinary procedure.

- Supporting contractual and commercial agreements.

Commercial and contractual disputes with customers, suppliers and partners may require detailed documentary support for their resolution. Many such interactions are purely electronic, so finding ways to preserve the terms and conditions, and dates of agreements can be extremely useful in averting losses and in successfully exploiting arbitration procedures and alternative dispute resolution.

- Proving the impact of a crime or dispute.

In many cases it may be necessary to show how much damage has been caused by an incident or criminal act. This may require evidence gathering in its own right, for example, logs to show downtime, records of staff overtime, costs of new equipment, and business lost.

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 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 [Melia 2002]. 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, including:

- Where is data generated?
- What format is it in?
- For how long is it stored?
- 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?
- To what business processes does it relate?
- 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, 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, and even voice over the Internet. Each of these may need preserving and archiving. A worst case scenario has some of this traffic encrypted.

The range of possible evidence sources includes:

- Equipment such as routers, firewalls, servers, clients, portables, and embedded devices;
- Application software, such as accounting packages for evidence of fraud, ERP packages for employee records and activities (e.g. in case of identity theft), system and management files;
- Monitoring software such as Intrusion Detection Software, packet sniffers, keyboard loggers, and content checker;.
- General logs, such as access logs, printer logs, web traffic, internal network logs, Internet traffic, database transactions, and commercial transactions;
- Other sources, such as CCTV, door access records, phone logs, PABX data, telco records and network records, call centre logs or monitored phone calls, and recorded messages;
- Back-ups and archives, for example, laptops and desktops.

The collection of evidence can also be put into two categories.

- “Background” evidence (data gathered and stored for normal business reasons).
- “Foreground” evidence (data specifically gathered to detect crime, or to identify criminals).

The gathering of foreground evidence is usually referred to as “monitoring,” as it typically involves analysing what people are doing by the real-time monitoring (e.g. IT or surveillance). Monitoring is generally regulated by laws such as those concerning privacy and human rights and while it is clearly necessary to monitor in order to fight crime, expert legal advice in the local country or jurisdiction is required to ensure it is done legally.

The strength of background evidence is sometimes founded in that it has been collected according to standard documented business procedures.

While the aggregation of evidence from the various sources will help the availability of evidence during an investigation, it may also become a potential vulnerability. The security of this data store will be extremely critical and should be subject to stringent technical and personnel security.

As Data correlation and event corroboration are desirable, this thorough examination of sources should allow any useful cross-correlations to be identified. Whether or not multiple sources will actually be collected will depend on the evidence requirement to be identified in step 3.

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 joining 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 [Ahmad and Ruighaver 2003]. The high-level audit policy proposed by Ahmad and Ruighaver corresponds in many respects to this evidence collection requirement.

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 whether it can be performed cost effectively.

- Can evidence be gathered without interfering with business processes?
- Can an investigation proceed at a cost in proportion to the incident?
- Can an investigation minimise interruption to the business?
- Can the evidence make an impact on the likely success of any formal action?
- Can the evidence be gathered legally without infringing employee rights?

The costs of the evidence gathering process that need to be taken into consideration when deciding how much potential evidence can be collected are:

- Cost of monitoring (including tools and staff-time);
- Cost of secure storage;
- Cost of organising potential evidence – by classifying, indexing and preparation;
- Cost and implications of retrieval if evidence is demanded by a court;
- Cost of investigations especially if external incident response team or forensic examination resources will be used.

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 any investigations.

In addition to the actual data, several other factors influence the utility, reliability and availability of potential evidence.

- Meta-data

Raw data is difficult to use as evidence out of context. The date and time of the creation and modification of a file can be critical in terms of providing evidence of an action and allowing it to be correlated with other forms of evidence, such as witness statements. Unfortunately, time stamps can be over-written and the clocks on PCs are often inaccurate. Cryptographic time-stamping services are available, along with network time synchronisation products which can help to alleviate this. Weight can also be given to data through the use of digital signatures to authenticate the creator (or sender) or recipient of a file. The use of hashes can similarly demonstrate the integrity of a file's contents.

- Corroboration and Redundancy

The various logs may each contain indications of the same event or activity. Duplication may provide a form of corroboration if, for example, independent monitoring detects similar activity or independent confirmation of the involvement of a suspect. Duplication also provides an element of redundancy should any evidence become corrupted, tainted or in some way inadmissible. There may also be instances where evidence collected over a period of time may lessen the need to perform a full-scale forensic analysis of a suspect's hard disk [Melia 2002]. For example, in the case of an employee, the evidence may be sufficient to encourage them to resign, if the employee knows that the organisation has seized his PC, which can provide corroboration of the evidence gathered through other means.

- Associations and Cause and Effect

Evidence should not only indicate what happened, but how, when and by whom. Various pieces of evidence may need to be linked to provide the causal link between the perpetrator and the damaging activity. Ahmad (2002) proposes a forensic chain-of-evidence model covering access control logs, source operating system event logs, network application logs, network traffic logs, and the target's operating system log. Associating events in the various logs allows a complete trace of how the incident took place and of the identity or location of the source. More recently there have been cases of not guilty verdicts based on concerns that Trojan horses may have been responsible, not the alleged perpetrator. Suitable evidence gathering might be able to show whether or not this was actually the case.

- Length of time of storage of data

In many instances the length of time data need to be kept is specified by regulators or law. Certain types of data need to be stored for differing periods of

time, depending on these rules. This should be specified in a data retention policy. Choosing how long to store data which may be of potential evidentiary value is a separate issue related to the cost and benefit assessment. A recommendation to store emails and firewall logs for a number of years is not atypical, if, for example, an organisation wants to be in a position to track the progression of a possible large scale fraud or to prove an employee's continued violation of corporate acceptable use policy. One particular issue is that of re-cycling back-up tapes. Much information is being lost each time a tape is re-used. The length of this cycle should be reviewed, bearing in mind the potential investigative and evidential value of any data being lost. Furthermore if there is an incident, it may be prudent to suspend re-use of back-up tapes to avoid loss of useful information or to show a court that there is no attempt to hide evidence.

- Size of Evidence

As well as the cost implications of gathering large-scale sources of evidence there is the issue of how to sift them, how to search them, and how to compress them. Yasinsac and Manzano (2002) recommend utilising data indexing and information fusion (e.g. products that allow multiple sources to be correlated). The organisation needs to consider data mining issues and how to summarise and categorise potential evidence.

- Hardware

Some hardware that may harbour potential evidence is not or cannot be routinely monitored, for example PDAs and mobile phones. There is a particular issue when someone leaves the organisation: Should the former employee's hard disk, laptop, mobile phone and PDA be preserved in any way in case a need to investigate arises?

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 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.

There are two preliminary checks to be made:

1) Can the evidence be gathered without interfering with business processes?
2) Can the evidence be gathered legally?

At this stage legal advice is required to ensure that 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[1]' 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;
- Staff should be told what monitoring is happening, except in exceptional circumstances.

Pemble (2003) gives an overview of a typical set of problems and suggests how they may be addressed in the UK.

Logs can be forged, and evidence can be manipulated or planted to incriminate others, so appropriate security measures are required. Remote logging should be used, as local logs are too vulnerable. Using the two together can expose attempts to hide or change evidence, for example, if there is a discrepancy between them or if one of them decreases in size. Tools which check file integrity, such as Tripwire, can also be used. Remote logging also enables a centralised repository to be assembled where broad investigations can be performed to look for correlations across multiple independent data sets. Secure logging tools are under development, e.g. based on IETF RFC 3195 known as syslog-reliable, [New and Rose 2001] which supports encrypted and authenticated event message delivery. Brezinski and Killalea (2002) have produced guidelines for system management staff for evidence collection and storage.

Physical security of data, such as in 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 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.

This step correlates to Point F, protect the evidence, of Yasinsac and Manazano (2001). They propose measures such as exercising rigid control over administrator access to

[1] Ad hoc opportunistic searches, without justification, for potentially incriminating activities or communication.

systems housing potential evidence, encrypting evidence files and any transfers, using strong integrity checking, and periodic audits. Physical security measures should also be considered, such as access control using card swipes (and accesses should be logged), safes, and multiple copies in different storage locations.

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. At all times it must be in a tamper-proof (or tamper-evident state). This corresponds to the use of evidence bags in the physical world. Access to the evidence is controlled and anyone requiring an evidence bag must sign it in and sign it back with the contents unchanged. In the parlance of investigators this is known as continuity of evidence (in the UK) and chain of custody (in the US). The chain of custody also includes records of who held, and who had access to, the evidence (for example from swipe control door logs). Ceresini (2001) gives an overview of implementation considerations including policies and procedures for maintaining the forensic viability of logfiles.

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 (Allen et. Al. 1999). 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, such as those where information is transmitted over networks, so that messages from EDI and email systems can be stored under the code.

The code is structured according to five principles of good practice for information management.

- Recognize and understand all types of information.
- Understand the legal issues and execute “duty of care” responsibilities.
- Identify and specify business processes and procedures.
- Identify enabling technologies to support business processes and procedures.
- Monitor and audit business processes and procedures.

These principles are reflected in the code in sections comprising:

- Information Management Policy;
- Duty of care;
- Procedures and processes;
- Enabling technologies;
- Audit trails.

Certainly, adherence to the code does not guarantee admissibility and it does not appear to have been tested in court, but it does attempt to define best practice. It covers issues such as “system planning, implementation, initial loading, and procedures for the use of a system including workflow.” It also discusses issues that relate to demonstrating that systems have been running properly in order to provide confidence in the integrity of potential evidence. 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. The likely admissibility and weight of any evidence gathered rests upon this document.

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, but this step is about making sure it can be used in the process of detection. By monitoring sources of evidence triggers that mean something suspicious may be happening can be detected.

The critical question in this step is when should an organisation be suspicious? IDS are commonly used to detect suspicious network events and penetration attempts and to alert system managers to the threat. Network staff will know what they are looking for and will set the IDS rules to trigger when certain activities happen. IDS provide real-time monitoring of a certain set of incidents, which are often linked to a real-time response from the company, such as a pager message. Honeypots are another device that can provide a trigger of a suspicious event and provoke a preliminary investigation. Event correlation (Chen et al 2003) can be used to meet the high level audit requirement discussed in step 3.

Auditing is commonly used to refer to the review of records after they have been generated. Security auditing tools can be deployed to analyse a range of data which can be reviewed on a near-real-time basis or in an annual security audit. The frequency of such auditing needs to be related to the business risk discussed above.

In monitoring and auditing, the types of activities recognised as suspicious will be different for different business needs. For example, a forensic accountant may look for specific patterns in financial data to trigger suspicion of fraud or theft. Content checking may be used, for example, to identify IPR leakage or data theft. A suspicious event might be multiple emails on a sensitive subject from a person who is not actually involved in the subject.

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 the sort of behaviour that IDS and Honeypots might be used to detect. This should be captured in a "suspicion" policy that helps the various monitoring and auditing staff understand what triggers should provoke suspicion, to whom to report the suspicion, whether heightened monitoring is required, and whether any additional security measures should be taken as a precaution.

What exactly is audited, and what counts as suspicious will vary with time. The suspicion policy needs to be updated as new IPR is generated, new business processes are implemented, and new business relationships need to be protected. The policy should also be influenced by corporate intelligence of the evolving threat and modus operandi that the organisation should be aware of.

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. 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 (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;
- The incident is reportable under a compliance regime.

Some threshold on the potential for damage could be used as an indicator of whether to escalate matters (see for example Endorf (2003)). Any information about the skill-level or intent of any miscreant, or indication of the target or vulnerability under threat is also required. In information security terms we might be looking for signs of:

- *Reconnaissance* – if a high level of skill or knowledge of sensitive resources is used, then consider escalating.
- *Compromise* – if an attack shows knowledge of the organisation, sensitive resources, or appears focused on a particular objective, then consider escalating. If unable to prevent in future (e.g. patch the vulnerability), then escalate.
- *Exploitation* – escalate, unless trivial or closed-down.

Before proceeding with escalation or calling out the Computer Security Incident Response Team (CSIRT), two further questions need to be answered to assess the impact on the organisation of the response itself:

- Can an investigation proceed at a cost in proportion to the size of the incident?
- How can any investigation minimise disruption to the business?

At the outset of an investigation it will be unclear what the impact of the incident is likely to be and the amount of effort needed to investigate it. When it comes to an actual forensic examination, organisations need ready access to the necessary skill sets within a CSIRT. If this involves buying in the skills from a specialist company, their skills need evaluating, as do the standards they follow, their professionalism and security. This needs to be done before an incident occurs or else the most convenient company, not the most effective, may get the work.

The escalation procedure drawn up under this step should involve a decision-maker, sometimes referred to as an investigation manager, who can decide on whether to call out the CSIRT and make business-critical decisions such as whether law enforcement need to be involved. A decision maker is also required in case it is necessary to shut down operational systems and to determine whether an emergency disconnect or a managed disconnect is appropriate for an on-line system.

At all times those involved should implement a “need to know” policy. 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.

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.

Some issues relevant to all staff if they become involved in an incident. Such general advice includes:

- Keep written (paper-based) notes which are dated, timed and signed;
- Report as necessary and only to those staff with a need to know;
- Do not use compromised systems (e.g. email);
- Know how not to taint evidence;
- Know what laws and regulatory principles to be aware of.

A wide range of staff will be involved with, impacted by, or responsible for, evidence and investigations. The following groups will require more specialised awareness training.

- 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 adviser;
- Senior Management (potentially up to board level)

After the escalation of an incident a multi-disciplinary team drawn from the above is likely to be convened. These staff may not know each other well or have a great deal of interaction on a day to day basis, but fast and effective teamwork is essential. They will have differing priorities and potentially different interpretations of company policy. Often there will be no clear lines of authority and extensive negotiation will determine the course of action. This will affect middle managers on a frequent basis and they will require support and training to understand the decision points, to make the right decisions, and to avoid tainting evidence or prejudicing a case. Role-play training is ideally suited to this scenario.

A key role for the organisation when a CSIRT is called in is the "liaison manager" or "incident handler." A CSIRT, whether internal or external, needs a single point of contact to manage communications with the organisation and to ensure that any requirements for facilities or resources to expedite the investigation are met.

Training may also be required to understand the relationships and necessary communications with external organisations that may become involved such as:

- Police (not necessarily local force, especially if defending against allegations from overseas, or if the organisation is multi-national);
- Other law enforcement authority (e.g. in the UK, Customs and Excise, Trading standards, Serious Fraud Office);
- Overseas prosecution authority or court;
- Trade Union / Staff Association representatives;
- Internal or external auditors;
- Regulatory authorities (e.g. Financial Services Authority, Information Commissioner, Bank of England);
- Customers, suppliers, partner organisations;
- Facilities management organisations (e.g. companies to whom IT or building security has been outsourced);
- The media.

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 [Endorf 2003]. 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 (support to the corporate memory so that even if there are changes in personnel it will still be possible to understand what has happened);
- To provide further evidence if required in the future, e.g., if no action is deemed necessary at this point, but further developments occur.

The following are possible components of a case file.

- Incident description – what happened? How was it detected?
- The hypothesis –how was the incident caused? Has the perpetrator been identified? located?

- The evidence – includes the location if an appropriate digital record is not included, paper files, details of interviews, signed witness statements, physical evidence, etc.
- The argument – shows that the evidence 'proves' the hypothesis
- The impact: damage or potential damage to the organisation – including any evidence to support the damage assessment.

The case file should be stored securely and subject to access control, as is the case for any evidence.

Two further issues arise during the writing-up process. The investigation may have found inculpatory evidence (indicating a person's guilt), it may also have found some exculpatory evidence (indication of innocence). A case is rarely "cut and dried." An organisation must have a clear policy for handling such exculpatory evidence. At some point such evidence could be the subject of a court disclosure order. Suppressing it may not be possible and may well be illegal. In practical terms it may be required if the conclusion of the investigation turns out to be wrong.

Digital evidence can be difficult for a non-specialist to read and understand. Thus, the case file should show how to present the evidence e.g. using visualisation tools and time-line analysis of the incident or of events leading up to it [Stephenson 2003a]. The evidence may have to convince lay-people on a jury.

Finally, if any mistakes or errors are made during an investigation they should not be covered up. Errors in the forensic process may weaken the evidence, but as long as what actually happened is honestly recorded, it may still be useful.

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 and member states in the EU [RAND 2003].

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;
- Any additional measures required.

A key issue for the organisation is, under what circumstances should law enforcement be contacted? There is a need to be in contact with them in advance to understand their policies and priorities and how to work together effectively. Their willingness to prosecute may depend on:

- Severity of crime or scale of impact on the organisation;
- Amount of any financial loss;
- Whether the victim is potentially part of organised crime, or may look for further opportunities, or has demonstrated serious intent or a novel modus operandi to commit the crime;
- Manpower constraints and operational priorities.

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 put digital evidence into a business context and 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, particularly for middle managers who have to deal with an incident in a multi-disciplinary team.

Many organisations, as part of their general information security, incident response and crime prevention activities, will already perform some of the activities required to effectively collect and exploit electronic evidence. What is needed in most

organisations is a systematic and pro-active approach to the gathering and preserving of evidence to meet their business needs.

Possibly the most significant barrier to forensic readiness is that companies rarely communicate the business risks well enough to allow those who are monitoring the IT systems to collect the most appropriate data. The other main risk is that for a variety of unforeseeable reasons, evidence may be non-admissible or weakened by opposition lawyers. The field of digital evidence is new and courts are wary of accepting it. Best practice is still emerging and case law is thin on the ground.

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

A good example of where forensic readiness could be applied is e-voting. Most e-voting development has been concerned with the security of voting software and cryptographic protocols. What is also required for public confidence in e-voting is the ability to preserve evidence that the process worked as expected, and evidence of the output of the e-voting process.

A cautionary tale serves to illustrate the state of forensic readiness in one organisation. Wilding (2003) reports 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 had been installed and then given to another employee. His files on the fileserver had been removed and his mails on the mail-server had been deleted en masse. Back-up tapes potentially containing the files had been re-cycled. Email could not be retrieved. Remote access accounts were kept active. His desk had been cleared. Forensic readiness would allow an organisation to avoid these mistakes.

Finally, this paper has shown that forensic readiness has benefits for business, but law enforcement will also gain from its widespread implementation. In many cases corporate systems are the eyes and ears of high-tech police. Organisations that understand the digital evidence process can establish an effective relationship with the relevant law enforcement agencies. With their co-operation, law enforcement agencies will have a better chance of understanding the scope, scale, and nature of hi-tech crime, and obtain the evidence they need to prosecute it successfully. Forensic readiness provides a win-win scenario for business and law enforcement.

References

ACPO; Good Practice Guide for Computer based Electronic Evidence, Association of Chief Police Officers, Retrieved 4th November 2003 from www.nhtcu.org/ACPO%20Guide%20v3.0.pdf

Ahmad, A., Ruighaver, A.B., Improved Event Logging for Security and Forensics: Developing Audit Management Infrastructure Requirements, ISOneWorld, Las Vegas, USA, April 2003; Electronic version retrieved 14th November 2003 from http://www.dis.unimelb.edu.au/staff/atif/ISOneWorld.pdf

Ahmad, A., The Forensic Chain of Evidence Model: Improving the Process of Evidence Collection in Incident Handling Procedures, Proceedings of the 6th Pacific Asia Conference on Information Systems, Tokyo, Japan, 2-4 Sept, 2002; Electronic version retrieved 14th November 2003 from http://www.dis.unimelb.edu.au/staff/atif/AhmadPACIS.pdf

Allen. R, Dyer B, Galbraith I, Mayon-White B, Peggram R, Shipman A, and Smith M.; Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically, British Standards Institution, DISC PD0008:1999

Brezinski D. and Killalea T. Guidelines for Evidence Collection and Archiving, RFC 3227, February 2002, Electronic version retrieved 17th December 2003 from ftp://ftp.rfc-editor.org/in-notes/rfc3227.txt

Carrier B. and Spafford E. Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence Vol 2, 2, [Electronic version] Fall 2003

Ceresini T., Maintaining the Forensic Viability of Log Files; May 2001; Electronic version retrieved 17th December from http://www.giac.org/practical/gsec/Tom_Ceresini_GSEC.pdf

Chen K., Clark A., De Vel O., and Mohay G. ECF – Event Correlation for Forensics; [Electronic Version] Proceedings of the 1st Australian Computer, Network and Information Forensics Conference 2003

Endorf C., Running an IT Investigation in the Corporate Environment; 2003, Electronic version retrieved 17th December from http://www.giac.org/practical/GSEC/Carl_Endorf_GSEC.pdf

ENFSI; Guidelines for Best Practice in the Forensic Examination of Digital Technology, European Network of Forensic Science Institutes, October 2003

Jones A. and Sutherland I. Threats to Information Systems and the Way We Deal With Them, Information Security Bulletin, Vol 8 Issue 4, May 2003

Melia J. Linkin' Logs to Fraud, Security Management On-line, November 2002, Electronic version retrieved 17th December 2003 from http://www.securitymanagement.com/library/001335.html

New D. and Rose M. Reliable Delivery for Syslog; RFC 3195, November 2001, Electronic version retrieved 18th December 2003 from http://www.faqs.org/rfcs/rfc3195.html

Patzakis J., New Accounting Reform Laws Push For Technology-Based Document Retention Practices, International Journal of Digital Evidence Vol 2, Issue1, [Electronic version] Spring 2003

Pemble M. Email and Web Abuse – Monitoring and Investigations, Computer Fraud and Security, Volume 2003, Issue 7, [Electronic version] July 2003

RAND Europe; Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, Study for the European Commission Directorate-General Information Society/C4 (2002)

Schultz and Shumway, Incident Response, New Riders, 2002

Sommer P. Intrusion Detection Systems as Evidence, Recent Advances in Intrusion Detection 1998, RAID98, Electronic version retrieved 17th December 2003 from http://www.raid-symposium.org/raid98/Prog_RAID98/Full_Papers/Sommer_text.pdf

Stephenson, P. End-to-End Digital Forensics [Electronic version]. Computer Fraud and Security Vol 2002, Issue 9

Stephenson P., (2003a) Using Evidence Effectively, [Electronic version] Computer Fraud and Security Vol 2003 Issue 3

Stephenson, P. (2003b) A Comprehensive Approach to Digital Incident Investigation; to appear in Elsevier Information Security Technical Report

Tan, J. Forensic Readiness, July 2001, Electronic version retrieved 14th December 2003 from http://www.atstake.com/research/reports/acrobat/atstake_forensic_readiness.pdf

Tan, T., Ruighaver T., and Ahmad A. Incident Handling: Where the need for planning is often not recognised [Electronic Version] Proceedings of the 1st Australian Computer, Network and Information Forensics Conference 2003

Wilding, E. Lost Opportunities [Electronic Version] Computer Fraud and Security Vol 2003, Issue 1

Wolfe H. Evidence Analysis, Computers and Security Vol 22 (4), May 2003

Wolfe-Wilson, J and Wolfe, H.B. (2003) Management strategies for implementing forensic security measures [Electronic version]. Information Security Technical Report Volume 8, Issue 2, June 2003, pp55-64

Yasinsac, A. and Manzano, Y. (2001) Policies to Enhance Computer and Network Forensics. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. United States Military Academy, West Point, NY, June 2001

About the Author

Dr Rowlingson is a principal consultant in information security at UK company QinetiQ (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). 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.

Dr Rowlingson has a Ph.D in general relativity from the University of Aston in Birmingham. His hobbies include travel, golf, cricket, cycling, family, and friends. He can be contacted on rrrowlingsonNO@SPAMqinetiq.com.

Acknowledgements

The author would like to thank the CTOSE project partners and colleagues Paul Smith, Mike Stubbings, Paul Irwin, Phil Turner, Carolyn Nisbet, Dave Bacon and Pat Burke for their feedback and encouragement.