



CERTIFIED DIGITAL SECURITY FORENSICS READINESS PLANNING GUIDANCE DOCUMENT

THIS DOCUMENT OUTLINES THE PRINCIPLES TO CONSIDER WHEN PRODUCING A FORENSIC READINESS PLAN TO ENABLE AN ORGANISATION TO REACT POSITIVELY TO A SECURITY INCIDENT.



THIS DOCUMENT CAN BE USED TO HELP AN ORGANIZATION DEVELOP ITS SECURITY POSTURE AND IS GIVEN OPENLY TO THE COMMUNITY. AN ORGANIZATION SHOULD NEVER BE ASKED TO PAY FOR ANY IMPLEMENTATION GUIDANCE DOCUMENT ISSUED BY CDS. THEY MAY PAY FOR ADVICE AND CONSULTANCY TO IMPLEMENT THE VARIOUS ASPECTS OF THIS STANDARD, BUT THAT IS FOR THE ORGANIZATION TO ARRANGE WITH ITS CONTRACTORS.

TO MEET THE CERTIFIED DIGITAL SECURITY (CDS) STANDARD, AN ORGANIZATION MUST PROVIDE EVIDENCE AS TO HOW THEY MEET AND COMPLY WITH THIS GUIDANCE DOCUMENT (AN EXTRACT OF THE CDS MASTER STANDARD).





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 Digital Forensics Investigator 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 log files, 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;





Certified Digital Security Forensic Readiness Planning Guidance

- 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'.





Certified Digital Security
Forensic Readiness Planning Guidance

Index

Introduction2
Forensic Readiness.....5
Updates and Support6





FORENSIC READINESS

Digital evidence is required whenever it can be used to support a formal process. An organization 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 maximize an organization'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 organization 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.

The organization must have a plan in place outlining:

The organisations objectives of forensic readiness

A clear statement of what the company hopes to achieve after a security incident.

A clear statement of what it considers the threats to the business are, and what parts of the organisation are vulnerable.

Who will be responsible for the coordination of any response should the plan be called upon and be identified by post rather than an individual name

This nominated post must have a clear set of terms of reference and plan to work from

This plan should be tested bi annually and annotated on the plan.

Contact details of how and when pre arranged outside forensic support can be obtained that will include contracted response times and provision of post incident support (for example evidence giving). Confirmation of details should be tested bi annually and annotated on the contact sheet.

How evidence should be stored safely, how it should be handled to ensure its integrity and the need of an audit trail of the handling of evidence should this not be a part of the contracted out process.

Include a decision tree as to when to escalate a minor investigation to full formal event that may or may not include law enforcement.





Certified Digital Security Forensic Readiness Planning Guidance

Specify the offences when a full formal investigation (which may use the digital evidence) should be launched that should be handled by law enforcement e.g. Fraud, Paedophilia.

Include contact details of local law enforcement agencies as a source of information and assistance and as a point of contact for the reporting of offences.

The Forensic Readiness Plan should be stored as a hard copy - it may be impossible to access the online copy of the plan in the event of a network attack or system loss, and details of your forensic response may assist an attacker.

Contact details for the organization's forensic investigator should be held separately from the plan.

UPDATES AND SUPPORT

While this is a static document, the area of Digital Security is constantly changing. Readers are encouraged to check the CDS website (www.certifieddigitalsecurity.com) for:

- Updates to this and other parts of the standard.

- Downloadable blank forms for various aspects of the tasks necessary to secure a network, organization or business.

- Links to various organizations that will assist the organization achieve the standard necessary to achieve their target CDS level.

