Digital Forensics

Digital Forensic Readiness (DFR)

Prof HS Venter
hventer@cs.up.ac.za

Copyright © HS Venter (2015)

Contents

• Background (Rowlingson, 2004)
• Digital forensic readiness – definitions
• Rowlingson’s steps for DFR

• (Note that all references in the slides of this course are part of the course content and can be found on Google Scholar or the UP Library system)
Background

- Digital forensic investigations (DFIs) are commonly employed as a post-event response to a serious information security or criminal incident
- The DFI process is then followed to investigate the event/incident
- The problem: The DFI 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
- The quality and availability of evidence is an important aspect of the DFI
- This evidence may be collected in advance of a crime or dispute, and can be used to the benefit of the collecting organisation
• In a business context however, there is the opportunity to actively collect potential evidence in the form of:
  – log files
  – emails
  – back-up disks
  – portable computers
  – network traffic records
  – telephone records
  – much more…

• 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
  – It could lend support to internal disciplinary actions
Background

• Digital evidence could help manage the impact of some important business risks:
  – 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 sign “Trespassers will be prosecuted.”

Digital forensic readiness

• Part of a risk management process
• The business requirement to gather and use digital evidence has been recognized
• Six categories of policies to facilitate DFI (Yasinsac and Manzano, 2001)
  – Retaining Information;
  – Planning the Response;
  – Training;
  – Accelerating the Investigation;
  – Preventing Anonymous Activities;
  – Protecting the Evidence.
Digital forensic readiness

- Tan (2001) 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.

Digital forensic readiness Issues

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 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 log files;
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 log files 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.
Digital forensic readiness Definitions

• Managing/administering computer systems to make it easier to conduct a digital forensic investigation when needed
• 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 and to save cost

Digital forensic readiness Definitions

• 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
• The ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation (Rowlingson, 2004)
Digital forensic readiness Cost
Benefits – Motivation

• Must be able to show ROI
• Traditionally a Risk Assessment action
  – ISO27002
  – But not all risk in DFI will be identified
  – Need to identify the assets, though
  – Always a residual risk that remains
  – What about the insider threat?
• Having a DFI capability may be a sufficient deterrent for the insider threat

Digital forensic readiness Cost
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
• 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
Digital forensic readiness Cost Benefits

• 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)

• Can extend 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

Digital forensic readiness Cost Benefits

• 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).
Digital forensic readiness Activities where costs will be incurred

- There will be initial cost involved:
  - 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.

Examples of incidents where one has to deal with digital evidence

- Threats and extortion;
- Accidents and negligence;
- Stalking and harassment;
- Commercial disputes;
- Disagreements, deceptions, & malpractice;
- Property rights infringement;
- Economic crime e.g. fraud, laundering etc;
- Content abuse;
- Privacy invasion and identity theft;
- Employee disciplinary issues.
**Wide range of staff that can be involved**

- 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 or customer claiming infringement of an act, e.g. data prot. act);
- Staff (e.g. colleagues under investigation);
- Corporate security;
- IT staff;
- Legal advisers

**Wide range of external parties that can be involved**

- Police (even cross-jurisdictional);
- Other law enforcement authority (e.g. Customs);
- Overseas prosecution authority or court;
- Trade Union / Staff Association representatives;
- Internal or external auditors;
- Regulatory authorities (e.g. SARS, banks…);
- Customers, suppliers, partner organisations;
- Facilities management organisations (e.g. IT or building security that has been out-sourced);
- The media – due to the need to manage the PR impact of any incident.
Goals for digital forensic readiness

• Must facilitate a practical implementation
• Goals of forensic readiness:
  – To gather admissible evidence legally
  – To minimise interruption to the business
  – To gather evidence that may adversely impact an organisation
  – To allow an investigation to proceed at a cost in proportion to the incident
  – To ensure that evidence makes a positive impact on the outcome of any legal action

Digital forensic readiness steps

• Rowlingson outlines 10 steps to accomplish digital forensic readiness…
1. Defining business scenarios that require digital evidence
   – Not possible to define all possible scenarios
   – Benefits of defining such scenarios:
     • A reduction in the impact of computer crime
       – Enhance awareness to reduce impact
     • Legal requirements
       – Making sure evidence is stored in a legal way
       – So it does not disrupt workings of organisation
     • Production of evidence
       – To meet regulatory requirements

2. Identify different sources and different types of potential evidence
   – May help highlight gaps in the way information is currently being collected
   – Issues to consider: format of data, period of time it is stored, storage locations, control over stored data, other sources of information that may be required
3. Determine the evidence collection requirements

- Determine the type and range of information that could be collected
- Issues to be addressed:
  - How can evidence be collected without undue interference with organisation’s working processes?
  - Cost of investigation in proportion with magnitude
  - Legality of collecting required information
  - Is there sufficient info for successful investigation?
  - Economically feasible to collect said information?

4. Establish capability for legally and securely gathering and storing evidence

- Plan to make sure tools & facilities are in place
- Staff should be suitably trained to be
  - Aware of the requirements
  - Have practical experience in such procedures
- Issues involved:
  - Info collected in a manner that is legally sound?
  - Info stored in a manner that is admissible in a court?
  - Collect info legally, i.e. may they monitor/collect email?
  - Which members of the staff have access to records?
Rowlingson’s 10 steps to accomplish digital forensic readiness

5. Establish policy for secure storage and handling of potential evidence and ensure it is properly and regularly tested
   – Planning in advance
   – Ensure stored info not modified/tampered
   – Info stored in physically secure way

6. Detect & deter major incidents
   – Actually part of normal security processes
   – Fraud activity detected by pattern deviation
   – Leaking of IPR via email attachments/docs
   – Abuse of privileges detected by changes in individual’s authorities & access rights
   – Cannot monitor/detect everything! Why?
   – Investigator should use own discretion
7. Specify circumstances in which incident should be escalated to full investigation
   - Ensure policies for incident management is adequate to know when to escalate incident
   - Which individuals should be informed?

8. Train all relevant staff in incident awareness
   - All staff involved will then know their role
   - Will have understanding of legal requirements
   - If process started, too late to train staff then!

9. Document case describing impact
   - This provides template for future incident
   - Allow managers to observe/reflect impact

10. Have procedures legally reviewed
    - Organisation will then have confidence that steps implemented are effective and correct
    - Sought legal advice
Conclusion

• DFR 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 DFR 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 DFR capability

Conclusion

• Forensic readiness is complementary to, and an enhancement of, existing InfoSec activities
  – It should be part of an risk assessment
  – Closely related to incident response and BCP
  – Part of security monitoring
  – Incorporated into security training
• DFR has benefits for business, but law enforcement will also gain from its widespread implementation
References


Assignment 1

- Choose any real business out there.
- Write ½ page what the business scenario looks like.
- Write a high-level DFR proposal for the business.
- 3 Pages Max (including business scenario)
- Marks:
  - Structure: 5
  - Content: 15
- Deadline: Friday 14 August 2015, 9:00 sharp
- NO late uploads accepted. Claiming systems were slow etc will not be accepted.
- PDF submission only: Studentno_Assignment1.pdf