Ensuring legal admissibility and managing disclosure of electronic records

Pro-active Strategies

Peter Sommer

London School of Economics

peter@pmsommer.com

p.m.sommer@lse.ac.uk

LSE

Pro-active strategies

- **The conference theme appears to be "admissibility and disclosure" – is this enough?**
- **The broader context: to prevail under legal challenge – and at reasonable cost**
- **Main reason for forward-planning: emergency actions are often inadequate and very expensive**

LSE

Pro-active strategies

Strategy has to encompass:

- **Admissibility Tests**
- **Practical Mechanics of Disclosure: CPR31**
- **A "witness" who can attest to reliability and completeness**
- **Potential problems and practical resolution of "inextricably linked":**
  - **Privileged material**
  - **Confidential material**
  - **DPA conflicts**
  - **RIPA conflicts**

LSE

Pro-active strategies

Two apparent alternative routes:

- **Certification of compliance with appropriate standards**
- **Forensic Readiness Program**

(in fact they can complement each other)

LSE

Standards Compliance

- **BIP 0008-1: Code of practice for legal admissibility and evidential weight of information stored electronically**
- **BIP 0008-2: Code of Practice for Legal Admissibility and Evidential Weight of Information Communicated Electronically**
  - ➔ **Emails, SMS, IMs, web-services, EDI**
- **BIP 0008-3: Code of Practice for Legal Admissibility and Evidential Weight of Linking Electronic Identity to Documents**
- **BIP 0067:2006: A guide to developing a retention and disposal schedule for business information**
- ***and associated work-books***
- **ISO 15489: Records Management**

LSE

Standards Compliance

Reasons for aiming for Standards Compliance:

- **Process is likely to identify a wide range of deficiencies which can then be corrected**
- **May be useful (or essential) contractually as defining expected service standards**

LSE

Standards Compliance

Typical discovered deficiencies:

- No information policy document
- No retention schedule
- Inappropriate / inadequate security controls
- Lack of procedural documentation
- Insufficient control of document input procedures
- Insufficient information about the technology from the system supplier

LSE

Standards Compliance

Typical discovered deficiencies:

- lack of documentation on audit trail content and access procedures
- use of inappropriate facilities, such as image clean-up or “deletion” facilities
- no thought of future migration requirements

LSE

Standards Compliance

Limitations of Standards Compliance

- Standards do not absolutely guarantee admissibility or acceptability for weight
- Standards are inevitably generic – may not cover everything you really need and may also ask you to spend much time explaining and justifying why some aspects are irrelevant
- Can be disproportionately costly and disruptive
- Introduces a box-ticking approach over more fundamental analysis (if done badly)

LSE

Standards Compliance

Limitations of Standards Compliance

- Rather useless if nearly all detailed activity is left to outside consultants
- Can produce a false sense of security
- May omit important informal records
  - → PCs, laptops, cellphones, PDA etc
- May not be especially persuasive in certain overseas jurisdictions
- May not deal effectively with the practical mechanics of disclosure, explanations to court, issues of inextricably linked material

LSE

Forensic Readiness Programs

Essentially:

- **Based on threat analysis / scenario development**
- **Requires identification of potential evidence / disclosure requirements – and plan for their formal production**
- **Results in a proper Contingency Plan – which is tested and kept up-to-date**

LSE

7-step Forensic Readiness Plan

Identify:

- the main likely threats/ legal challenges faced by your organisation
- what sorts of evidence / disclosure you are likely to need if you have to proceed to civil or criminal litigation
- what you will need to do to meet various regulatory and compliance requirements
- how far you may have that material already
- what you will need to do to secure additional essential material

LSE

7-step Forensic Readiness Plan

- the management, skills and resources implications for your organisation
- turn the results into an action plan – which will need regular revision as the organisation and its ICT infrastructure develops.

LSE

7-step Forensic Readiness Plan

The Good News:

quite a bit of the work may already have been carried out elsewhere in the organisation….

…….Disaster Recovery / Business Contingency Plans

LSE

Business Contingency Plans

- **Preparation against disaster:**
  - → Fire
  - → Flood
  - → Terrorism
  - → Denial of access
  - → Computer failure
  - → Etc etc

LSE

Business Contingency Plans

- **Tells organisation what to do:**
  - ➔ Emergency Priorities
  - ➔ Team that will act / Reporting Responsibilities
  - ➔ Migrated offices, locations
  - ➔ Migrated people
  - ➔ Migrated ICT
  - ➔ PR for customers, clients, investors, bankers, public-at-large etc

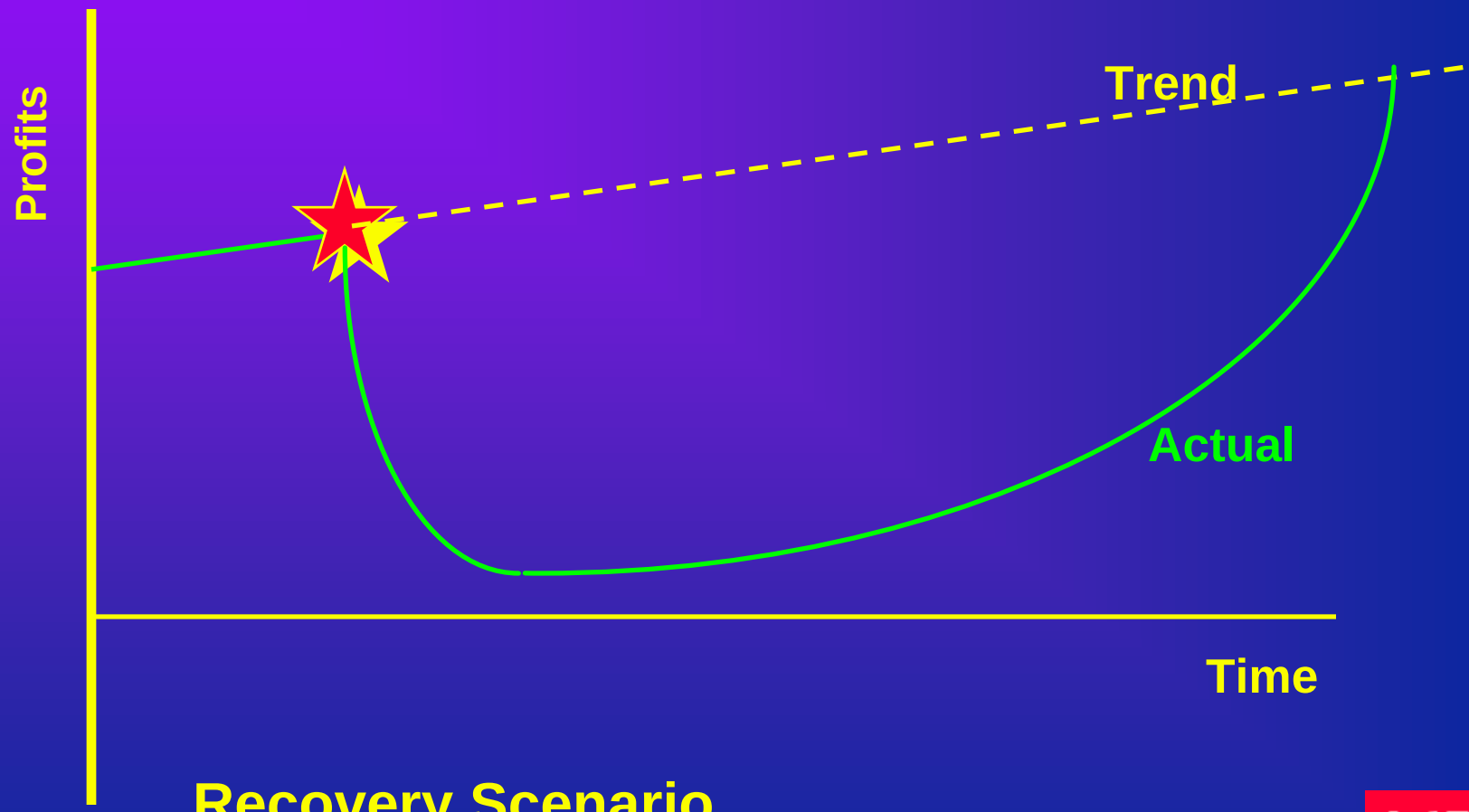
LSE

Consequential Loss

What happens to profits ...

LSE

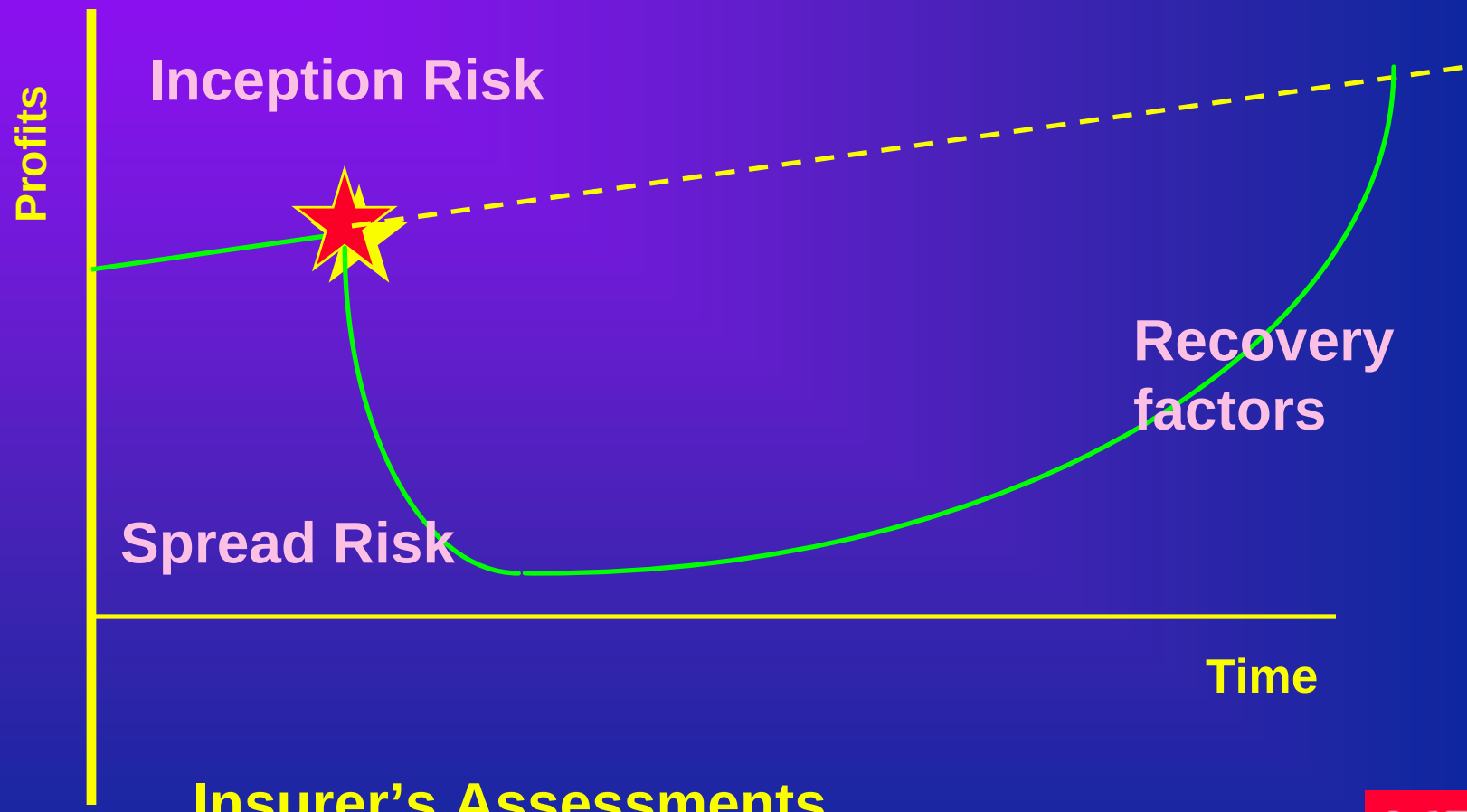
Consequential Loss



Recovery Scenario

LSE

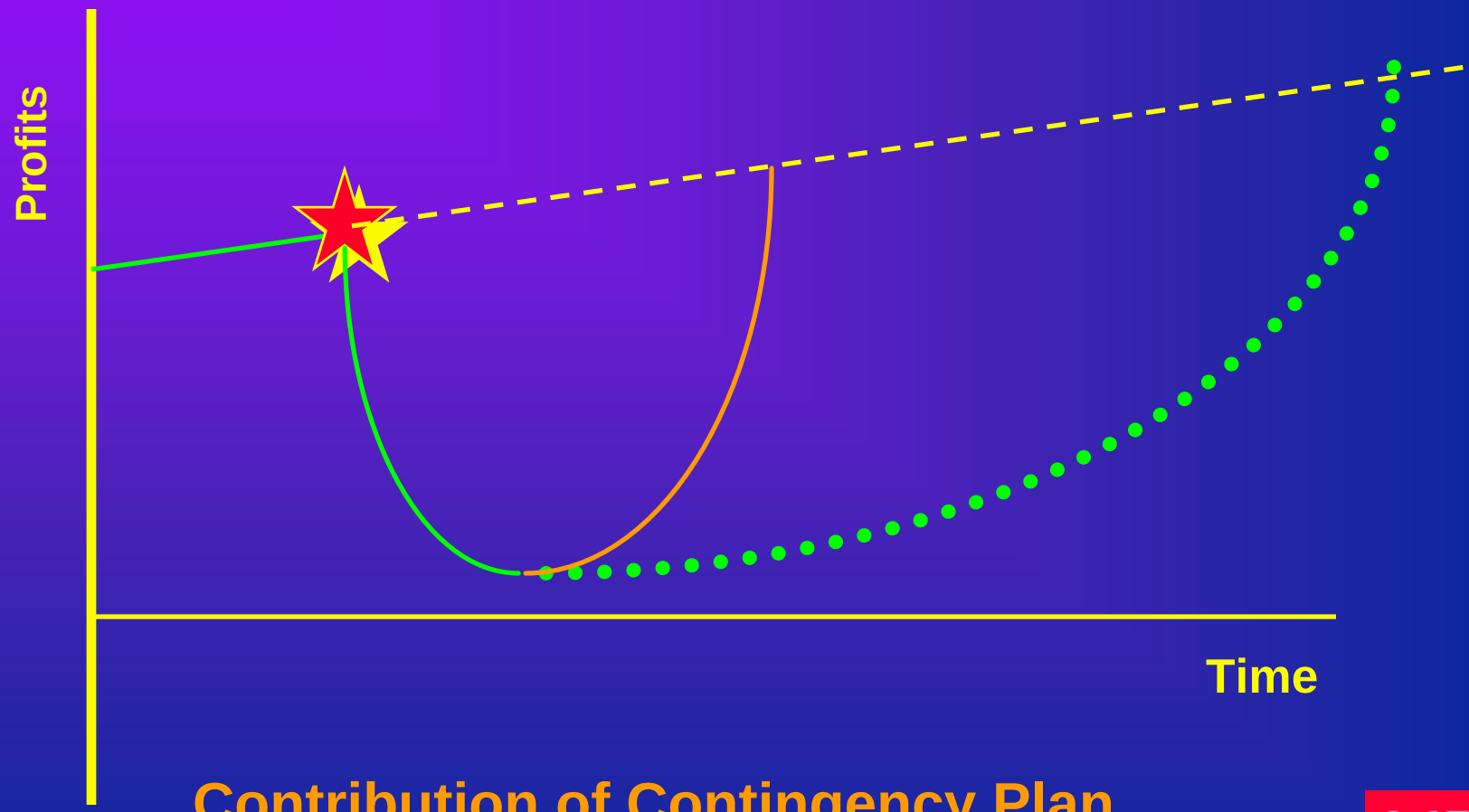
Consequential Loss



Insurer's Assessments..

LSE

Consequential Loss



Contribution of Contingency Plan..

LSE

Business Contingency Plans

Research, Design

- Business Analysis
  - → to determine priorities (it's too expensive to restore everything instantly)
- Relation of business processes to specific ICT resources, hardware, software, communications links; availability of back-up
- Detailed plan for who does what when
- Emergency Response Team
- Internally published Plan
- Frequent Testing and Revision

LSE

Business Contingency Plan / Forensic Readiness Plan

Research, Design

- Business Analysis
  - → to determine evidential and disclosure needs
- Relation of business processes to specific ICT resources, hardware, software, communications links; availability of back-up
- Detailed plan for who does what when
- Reporting requirements
- Internally published Plan
- Frequent Testing and Revision

LSE

Forensic Readiness Plan: Additional Requirements

- Legal / Regulatory requirements
- Analysis of back-up plans
  - ➔ Incremental / complete
- Specific Data Retention / Destruction requirements
- Decisions about mode of disclosure
  - ➔ Electronic, print-out, extents, etc
- Witness to explain systems, material produced, testify to reliability and completeness

LSE

Reliability/ Weight Persuaders

- What does the system do?
- What are the inputs and outputs?
- How long has it been in existence?
- What record is there of failures and glitches?
- If there were failures – what would they look like?
- What security precautions are in place?
- Is there a distinct audit process?
- How specifically has an exhibit or disclosure been produced?
- What is meant by “complete”?

LSE

Forensic Readiness Plan: Additional Requirements

- **Anticipation of "inextricably linked" material:**
  - → Privileged material
  - → Confidential material
  - → DPA conflicts
  - → RIPA conflicts
  - → Employee and 3rd party rights

Eg email databases, other databases, forensic recovery situations

In specific situations may need negotiation, appointment of trusted third party, Single Joint Expert

LSE

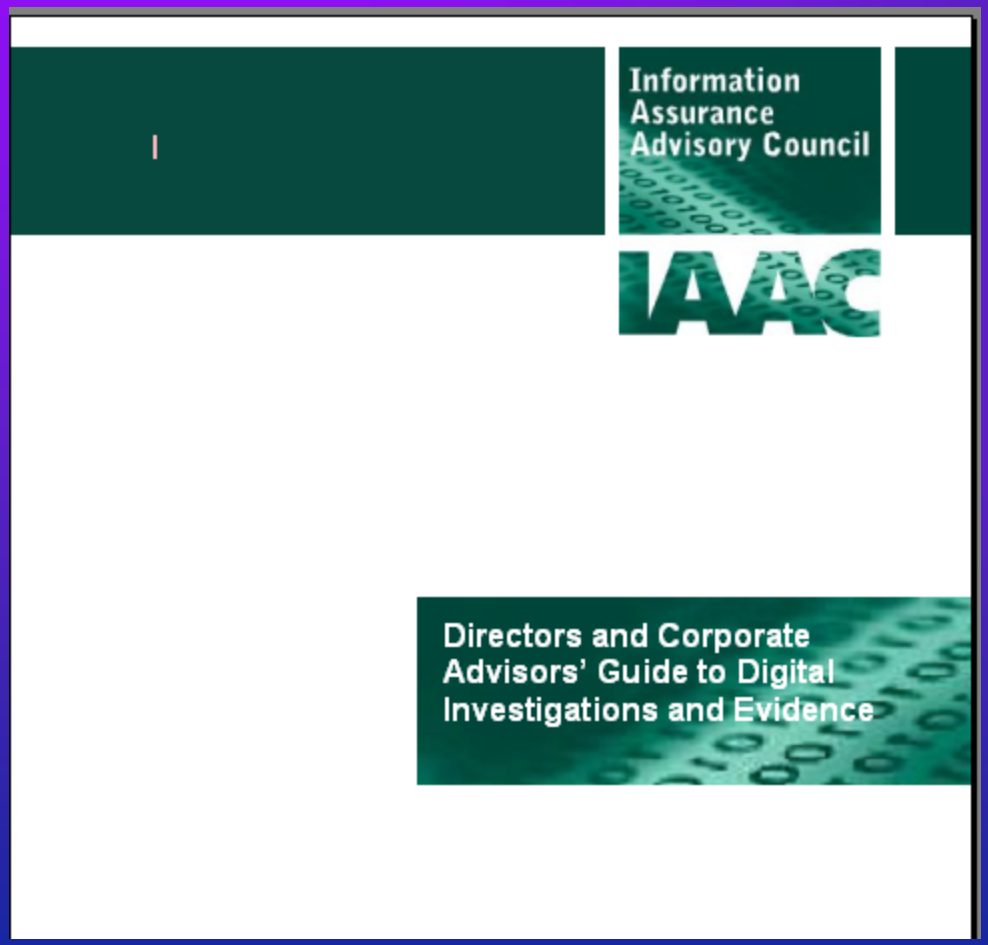
Forensic Readiness Plan: Additional Requirements

- **Informal Sources**
  - → apparently insignificant items of hardware which may be drawn into disclosure / have evidence
  - → Laptops
  - → Cellphones, PDAs
  - → Telephone records
  - → Home PCs
  - → External hard-disks, USB st

Likely to be significant arguments about privilege, privacy, DPA, RIPA etc

LSE

Guide to Digital Investigations and Evidence



First published 2005; new edition due

www.iaac.org

LSE

Forensic Readiness Plan

Who prepares?

- You can use consultants / templates / standards work-books to assist
- But in the end responsibility must devolve to a senior full-time employee of the organisation

LSE

Forensic Readiness Plan

Why have plan?

- To reduce costs and panic
- External consultants will have to “learn” the business
- Lawyers will have to identify admissibility and privilege issues on the spot
- Can also be used for other legal situations, eg internal disciplinary disputes, routine transaction disputes, to aid law enforcement

LSE

Pro-active strategies

- **Compliance with standards and legalistic concern with the problems of admissibility may not be enough**
- **The broader context: to prevail under legal challenge – and at reasonable cost**
- **Main reason for forward-planning: emergency actions are often inadequate and very expensive**

LSE

Ensuring legal admissibility and managing disclosure of electronic records

Pro-active Strategies

Peter Sommer

London School of Economics

peter@pmsommer.com

p.m.sommer@lse.ac.uk

LSE