

# MANAGING RISK

## LAW FIRM RISK MANAGEMENT

Published by Web4Law Ltd  
www.web4law.biz

# Lexcel Practice Excellence Kit Launched

## Law Society publishes the third edition of the Lexcel Practice Excellence Kit

Web4Law has been heavily involved with the production of the new Practice Excellence Kit, now on sale from Law Society Publishing.

A team of specialists from the company prepared the new Office Procedures Manual while Director, Matthew Moore, is one of the principal authors of the new Assessment Guide. This is the third edition of the Kit that Matthew has been involved in, and the first under the Web4Law banner.



Lexcel Practice Excellence Kit

This new edition reflects the new Lexcel Practice Management Standards, which are now in force. Key changes to Lexcel include:

- new sections dealing with policies, client care and supervision, and risk management;
- coverage of the latest issues such as computer use and combating money laundering;
- removal of the need for documented procedures for a number of provisions where compliance can be demonstrated by other means.

The *Lexcel Practice Excellence Kit* contains:

- The *Lexcel Office Procedures Manual* – which provides a series of useful templates from which solicitors can prepare a manual for their firm. An accompanying CD-ROM helps to tailor the office manual to firms' requirements.
- The *Lexcel Assessment Guide* – which sets out the requirements for meeting the revised Lexcel Practice Management Standard and explains the process of Lexcel certification. This edition also includes the authoritative assessor's guidelines.

It is encouraging to report that initial reaction to both the new version of Lexcel and the revised publications has been largely positive. We look forward to reporting further

continued on P3

## Disabled Web Access Ignored

*A study of 1,000 web sites across the UK shows that most organisations breach guidelines on making sites accessible to disabled users and risk legal action under disability discrimination laws.*

Since March 2003, the Disability Rights Commission (DRU) and the Centre for Human Computer Interaction at London's City University have been testing sites for technical compliance with the World Wide Web Consortium's Web Content Accessibility Guidelines (WCAG).

Of the 1,000 sites tested, 808 (81%) failed on automated testing to reach the minimum standard for accessibility, known as Level A. The testing involved running commercially-available software against each of the 1,000 sites. Only 100 of the sites tested were subjected to additional manual tests by a disabled user group comprising individuals with dexterity impairments, dyslexia, hearing impairments, blindness or partial sight.

Other than a failure to describe images, the disabled user group found other common problems: cluttered and complex page structures; confusing and disorienting navigation mechanisms; failure to describe images; inappropriate use of colours and poor contrast between content and background.

continued on P3

## IN THIS ISSUE

- E-Conveyancing Risk
- Managing Compliance Audits
- Money Laundering Tipping Off
- People – Asset or Risk?

## CONTENTS

In this issue:

### NEWS

|                      |         |
|----------------------|---------|
| News                 | Page 1  |
| Comment              | Page 2  |
| IT Risk News         | Page 4  |
| Conferences & Events | Page 16 |

### FEATURES

|  |         |
|--|---------|
| <b>Gearing up for Renewal</b><br>Janine Parker             | Page 5  |
| <b>E-Conveyancing Risk</b><br>Nicholas Bohm                | Page 6  |
| <b>Feature Interview</b><br>Nigel McEwen,<br>Tarlo Lyons   | Page 8  |
| <b>Compliance Audits</b><br>Ian Austen                     | Page 10 |
| <b>Money Laundering<br/>– Tipping Off</b><br>Matthew Moore | Page 11 |
| <b>Data Protection Risks</b><br>Peter Carey                | Page 13 |
| <b>Book Reviews</b>  | Page 15 |

**Editor: Rupert Kendrick LL.M**

Editorial, subscriber, advertiser and reprinting enquiries  
to the Editor *Managing Risk* at:  
Ebony House, 15, High Street, Sharnbrook, Bedfordshire  
MK44 1PG  
Tel: 01234 782810  
E-mail: rupert@web4law.biz

**Publisher: Web4Law Ltd** web address: [www.web4law.biz](http://www.web4law.biz)

**Copyright** Web4Law Ltd 2004. All rights reserved.  
Published by Web4Law Ltd. No part of this publication may  
be reproduced without consent. While every effort is made  
to ensure the accuracy of the information in this  
publication, no guarantee is expressed or implied and the  
publisher does not accept liability for any loss or damage  
arising from any errors or omissions occasioned by any  
person acting or refraining from acting as a result of any  
views (which are personal and not necessarily those of the  
publisher) expressed herein.

**Privacy Policy**

Web4Law does not sell or disclose the names or  
contact details of subscribers and is registered under the  
Data Protection Act 1998

## *From the Editor's Pen*

### People-based Risk Management...

The launch of the Lexcel Practice Excellence Kit is a timely reminder of the approaching professional indemnity insurance renewal 'season' for law firms. In fact, by the time the next issue of *Managing Risk* is published, the renewal date (1 October 2004) will have passed.

The latest edition – the third edition – introduces new sections which look specifically at policies, client care and risk management. It is interesting to see that risk issues for law firms are now increasingly concerned with the management of people – internally, through carefully formulated policies for the proper management of the practice – and externally, through management of its clients, with tailored client care programmes.

When analysing negligence claims and complaints against law firms, it is almost unheard of to encounter an allegation that the solicitor misinterpreted, or was ignorant of, the law. No – the problem invariably relates to the conduct of the lawyer – not the knowledge. And how often does the 'conduct' alleged go to the way in which the lawyer managed the people involved in the claim – as often as not, neglecting their interests?

Look at the contents of the revised sections of the Practice Management Standard. They include such key issues as: firm-wide policies; people management; supervision and client care. All these are 'people' issues – issues that require the management of people.

This is not the place to rehearse past mishaps in law firms, but there will be no lawyer reading this who will not have heard of the e-mail disasters occurring in (yes) some of the largest city firms, not to mention complaints of discrimination and the like within large practices. All these issues, although in some cases involving failures to observe office procedures, are fundamentally failures by lawyers to manage people.

The handling of 'people' is a management skill that is only just being recognised as a key area of risk for law firms, but it is likely to prove a costly risk area if it is ignored.

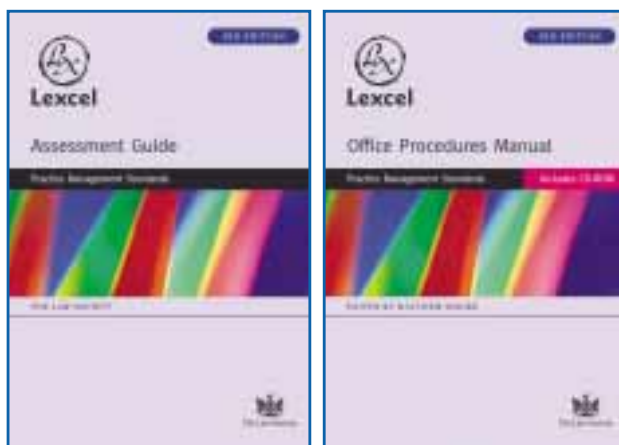
Rupert Kendrick LL.M  
Editor

**continued from P1**

on the implementation of Lexcel 2004 in future issues.

**Lexcel Training from Web4Law**

As reported in our Spring issue, Web4Law was delighted to win the tender for the delivery of training in the Lexcel Scheme for the Law Society. The courses are now well under way and consist of:

**Assessor and Consultants update**

This is a one day update course on the new provisions of Lexcel 2004 and Assessor practice and is provided in conjunction with representatives from the Lexcel Office.

**Practices Update**

Web4Law associate, Peter Warner – a consultant and assessor under the Lexcel scheme, is leading a half-day course showing practices what is necessary to

update themselves with Lexcel 2004.

**New Assessor and Consultants Training** Web4Law provides two of the three days of training for individuals who wish to be recognised by the Law Society as approved consultants or assessors under the scheme.

For further details of courses and information on availability please contact Richard Watkins at the Lexcel Office (020 7242 1222).

**Office Procedures Manual**

The contents have changed to reflect the revised sections of the Law Society's Lexcel Practice Management Standards, and include:

- firmwide policies;
- planning;
- financial management;
- facilities and information technology;
- people management;
- supervision and risk management;
- client care;
- case and file management.

**Assessment Guide**

The new edition also includes:

- assessors guidelines to help promote a better understanding of the assessment criteria;
- the full text of the revised Lexcel Practice Management Standards now in force.

The Assessment Guide was written by the Lexcel Office with particular input from Matthew Moore and Vicky Ling. •

**continued from P1**

In total, the disabled user group identified 585 accessibility and usability problems; but nearly half of these (45%) were not violations of any of the WCAG's 65 checkpoints – meaning that they could be present on any web site which conformed to WCAG guidelines at any level.

The research found an average of eight instances of the World Wide Web Consortium's guidelines being violated per homepage; but it also found that on average there were 108 potential instances on the typical homepage where a disabled person might be disadvantaged in his or her use of a site.

The **Disability Discrimination Act 1995** states that it is unlawful for "a provider of services" to discriminate against a disabled person in failing to comply with its provisions."

**Ignorance among developers**

Researchers canvassed the views of nearly 400 web site developers. The investigation found that levels of accessibility expertise among web developers were low with only 9% claiming any accessibility expertise. Only 9% of developers had used disabled people to test their sites.

Among those who commission web sites, the DRC found that 97% of large organisations (more than 250 employees) were aware of accessibility as an important issue, and 88% were aware of their responsibilities under the **Disability Discrimination Act**. But among SMEs, awareness of accessibility as an important issue dropped to 69% and only 48% reported awareness of the legal duty.

The DRC is appealing to developers to involve disabled users with a range of sensory, cognitive and mobility impairments from an early stage in the design process, and asking that they do not rely exclusively on automatic testing software. It recommends that web site commissioners should formulate written policies for meeting the needs of disabled people.

**Problems with WCAG**

Version 1.0 of the current Web Accessibility Initiative WCAG came out in May 1999. Version 2.0 is currently a working draft. City University conducted its research with reference to Version 1.0 and called for the WAI to revise its guidelines to encourage a reduction in the number of links on a site and to ensure that genuine and necessary links are clearly identified as such, to preserve links to the homepage, to improve search design, to eradicate excessively deep site

structures, and to ensure that page titles are informative.

**Legal action**

The DRC has decided against "naming and shaming" but has made clear that it finds the current state of web accessibility to be "unacceptable".

The DRC explained: "Our report contains a range of recommendations to help web site owners and developers tackle the barriers to inclusive design. However, where the response is inadequate, the DRC will not hesitate to use its legal powers – from 'named-party' Formal Investigations which can lead to sanctions against the owners of inaccessible web sites, to support for test cases brought by individual disabled people – to ensure the web becomes fully inclusive to disabled users."

Helen Petrie, Professor of Human Computer Interaction at City University, said: "In addition to better use of the Guidelines, the most effective thing web developers can do is involve disabled users in testing their web sites. This will not only improve accessibility but also usability for everyone – non disabled users were almost 50% slower when using low accessibility web sites in comparison to high accessibility sites." •

[www.out-law.com](http://www.out-law.com)

# IT Risk

*A round-up of the latest key IT risk issues*

## File Sharing Ignorance Threat

Findings from a UK survey commissioned by SurfControl, a leading Web and e-mail filtering company, reveal that businesses are leaving themselves exposed to risks by not managing the use of Peer-to-Peer (P2P) file-sharing. Many P2P communications could be leaving company networks wide open to virus attacks and copyright breaches by staff.

With responses from over 500 of the country's IT managers and HR officers, two thirds believe that their company 'takes P2P file-sharing seriously'. However,

the admissions made by the respective departments paint an altogether different picture. HR give staff the green light to file-share at work. Despite playing an intrinsic role in creating staff handbooks, almost half (49%) of the UK's HR officers admit that their company does not yet have a policy concerning the use of file-sharing in the workplace. A further 23% of HR officers 'don't know' whether their company has a policy to deal with employee file-sharing. Almost 50% of UK companies are without file-sharing security measures.



SurfControl – "businesses are leaving themselves exposed"

## Websense Research shows online Pornography

Websense, a leading provider of employee Internet management software, claims the number of pornography Web sites in the Websense URL database is more than 17 times greater than it was just four years ago

– surging from approximately 88,000 in 2000 to nearly 1.6 million sites today.

According to the National Research Council, an additional tactic known as "mousetrapping" is used by porn companies to redirect automatically surfers to another Web site when they attempt to leave an adult site. This redirecting can repeat dozens of times, and often leads to an increase in employee complaints and IT help-desk calls.

system patches, disaster recovery plans, etc, are robust and up to date;

- Respond to security incidents efficiently and effectively to minimise business disruption.

### Other headline findings

- One in three large businesses had their web sites attacked by hackers last year;
- Remote access and wireless network points are becoming the focus of security breaches;
- Unauthorised user access to computer systems is becoming an increasing headache;
- Increasing volumes of 'spam' are a growing concern for UK businesses;
- Employee Internet abuse is on the increase;
- The 'Blaster' virus topped the list as a virus epidemic sweeps UK businesses.

The threats associated with online pornography continue to be a significant problem for corporations; however, what is lurking below the surface in corporate networks can be equally as dangerous in the employee computing environment. For example, emerging threats such as viruses spread through P2P file sharing networks or infected attachments sent via instant messaging, while not as clearly visible a threat as online pornography, bypass normal security barriers and can leave companies exposed to hackers.

[www.websense.com](http://www.websense.com)

## DTI Information Security Survey 2004

The DTI Information Security Breaches Survey (2004), launched at Infosecurity Europe 2004 in April, headlined some key findings regarding information security:

- 74% of businesses (94% of large businesses) had a security incident in the last year;
- Malicious incidents have risen dramatically; 69% of companies (91% of large businesses) have suffered at least one such incident in the last year – up 44% from the 2002 survey;
- The average UK business has roughly one security incident a month and larger ones around one a week;
- The average cost of an organisation's most serious security incident was around £10,000 (£120,000 for larger companies) with the impact on availability being the biggest contributor to cost;
- Only 12% of respondents were aware of the contents of the internationally

recognised standard for information security – BS7799 and only one in ten companies has staff with formal information security qualifications;

- While spend on information security has increased, it is still relatively low and seen as a cost rather than an investment – companies spend an average of 3% of their IT budget on security compared with 2% in 2002 – still well below the 5-10% benchmark level.

### Recommendations:

- Draw on the right expertise to understand security threats and legal responsibilities;
- Integrate security into normal business practice, through a clear security policy and staff education;
- Invest appropriately in security controls to mitigate the risks or insurance to transfer them;
- Check key security defences, such as operating

# Gearing Up for Professional Indemnity Renewal

**Janine Parker,**  
**Assistant**  
**Director,**  
**HSBC**  
**Insurance**



**Brokers Ltd., examines some key issues for law firms to consider for this year's renewal**

**The 2004 renewal of professional indemnity insurance for the profession is rapidly approaching. Although the renewal date has been moved to 1 October 2004, the insurance market has already set rates and brokers are sending out proposal forms to practices.**

## Early deals

Some of the larger qualifying insurers are offering early renewal deals, but a practice should err on the side of caution when considering these. An early deal often means that the practice has to pay the first premium instalment up front. This should be to secure the quoted premium until the inception of the insurance policy.

I say 'should', as this was not my experience with one of my clients last year. My client has remained with the same qualifying insurer since the demise of the SIF and accepted an early renewal deal last year and, in good faith, paid the first premium instalment in July 2003. They then notified a claim with an estimated quantum of £150,000 at the beginning of August.

The qualifying insurer in question wanted to increase the premium and was reluctant to refund the first premium instalment. The outcome was a happy one and the insurer honoured the terms and the client renewed. But this scenario is not the only one to be considered when thinking of placing your indemnity early.

## 'Changing animal'

The insurance market during the solicitors' renewal season is a changing animal, Insurers begin to invite renewal at the beginning of the period but this does not mean those initial rates will be the rates at which the premiums are underwritten.

The profession is notorious for leaving the placement of their indemnity to the last moment; this trend pre-dates the open market renewal and dates back to the SIF (the majority of gross fee certificates being returned during the last week of August).

## Rates and risks

The rates for some insurers are dictated by what the rest of the qualifying insurers are quoting. Last year, one insurer quoted early and, two weeks later, another insurer entered the market quoting considerably lower rates.

*The key to obtaining the best premium is communication with your broker who will have been in communication with qualifying and excess layer insurers throughout the year and will know their game-plans for 2004*

Predictably, the first qualifying insurer reduced its rates to be in line with its competitor. By renewing too early, a practice could miss out on considerable savings. For example, the majority of risks were underwritten in the last two weeks of the renewal period.

One underwriting agency actually sent a letter to all their quoted practices advising that they were discounting 15% of quoted premiums. How would you feel if you had already renewed with them at the beginning of the season?

## Getting the best premium

The key to obtaining the best premium is communication with your broker who will have been in communication with qualifying and excess layer insurers throughout the year and will know their

game-plans for 2004.

I am not saying that early renewal offers should not be considered, but make sure that your broker undertakes a full market search at the end of the period to ensure you are paying the most competitive premium available.

The profession is becoming more commercial in its approach to purchasing indemnity insurance.

The practice understands that the cover does not differ from one insurer to the next. A broker should be instructed who specialises in solicitors' P.I, who can provide an excellent claims service, risk management advice and solutions, and will undertake a full search of the professional indemnity market at renewal.

## Factors to consider

When submitting professional indemnity submissions to the market, there are certain factors a practice must consider.

- Choose your broker wisely. What can your broker offer your practice? Do they have an exclusive facility and, if so, is that the only market they can approach or can they undertake a full market search on your behalf?
- Where is the location of your broker? If you are using a local broker, do they have knowledge of the London qualifying insurer market? Do they have direct links into these insurers or do they have to use a Lloyds broker to access the underwriters? If this is the case, how is the broker's commission being split? Would your practice receive a better service if you accessed the London broker direct?
- Is your broker providing your practice with alternatives to your existing arrangements? Do you know, for sure, that you are getting the best deal?
- *Do not flood the market.* You should always use one alternative to your current broker to make sure that you are accessing the right insurers. One insurer may have a very different appetite for your business than another. •

# Electronic Conveyancing – a new source of Risk

*Nicholas Bohm, solicitor,  
identifies some key risk  
issues that  
conveyancers will face in  
the electronic age*

**The Land Registry relies on signatures - the signatures of lawyers on applications, and the signatures of the parties on land transfers. In many cases, it has no means of verifying these signatures. It carries the risk of relying on a forgery, and is bound by statute to compensate the victim of the resulting error, or the victim of its rectification.**

The **Land Registration Act 2002** lays the foundations for electronic conveyancing. Documents such as applications and land transfers will be submitted in electronic form, with electronic signatures. These are different from paper signatures, with significant consequences for the incidence and nature of risk. The most likely form of electronic signature for electronic conveyancing is based on public key cryptography, sometimes called a digital signature.

### **Electronic signatures**

An electronic signature is the output of an algorithm applied to two inputs: the text or file to be signed, and the signatory's unique signature key (a numerical value). The electronic signature consists of a numerical value, contained either in a separate file, or in the signed document.

The usefulness of the signature depends on the fact that the unique signature key is associated with a unique verification key. The verification key can be used by another algorithm. The inputs to the verification algorithm are the text which purports to have been signed, the signature, and the verification key. The output is either a confirmation that the text or file was signed by the corresponding signature key, or a statement that no such confirmation can be given. A negative will result either if the signature was not made by the corresponding signature key, or if

the signed text has been altered in the slightest way after signing.

The signature key and the verification key are related to one another mathematically, but if they are properly created, it is computationally infeasible to derive the signature key from the verification key. A verification key can be provided to those who wish to verify a signatory's electronic signatures, or can be published without thereby revealing the signature key.

### **Risk implications**

The risk implications are significantly different from those of paper signatures. Electronic signatures are strongly bound to the signed text and the signature key, and that can be verified easily and with great confidence; but the binding of a signature key to a signatory depends on the willingness and ability of the signatory to maintain exclusive control of it. Paper

*The risk is the insecurity of the computers and networks used for electronic conveyancing.*

*The value exposed to the risk is the value of property which might be fraudulently transferred by the misuse of an electronic signature*

signatures are strongly bound to their makers, who cannot transfer or lose control of them; but they are not strongly bound to their text which can be altered without affecting the signature, and the reliability of their verification depends greatly on the time and effort a verifier chooses to expend on examining them to detect forgery.

The improved ease and certainty of the verification of electronic signatures is attractive; but their value depends on the extent of the obligations which the publishers of verification keys are prepared to accept in relation to the control of the corresponding signature

keys. No such obligations attach to paper signatures and those using electronic signatures are therefore entering a new field of risk.

### **Risk types**

The risk is the insecurity of the computers and networks used for electronic conveyancing. Malicious third parties may make secret copies of signature keys, or gain access to computers, or corrupt computers so that they sign documents without their user's awareness. Firewalls, intrusion detection systems, anti-virus software, and smartcards, provide some defence against such attacks, depending on the sophistication of their deployment, but the risks to the security of valuable signature keys remain substantial. The value exposed to the risk is the value of property which might be fraudulently transferred by the misuse of an electronic signature.

Those who publish verification keys would therefore be most unwise to accept that they must be deemed to have made any signature that can be verified by the use of the key – an absolute warranty of liability. The most that could wisely be offered would be an undertaking to use reasonable efforts to maintain the security of the private key; and even an undertaking to extend that to "all reasonable efforts" would be to promise something that few could in practice achieve.

### **Uncertainty**

Verifiers relying on such a qualified warranty are left with uncertainty. A verifier who meets a denial of responsibility for a successfully verified signature would be left to prove that the purported signatory failed to use reasonable efforts to protect the signature key - not an easy task. The Land Registry is driving forward the use of electronic signatures, and if the technology available for their deployment cannot eliminate the risks, it seems not unfair that they should carry those risks. •

*Nicholas Bohm is Electronic Commerce Consultant to Fox Williams and a member of the Law Society's Electronic Law Committee  
nbohm@ernest.net*

# DO YOU NEED A CYBER-RISK AUDIT?

Assess your firm's vulnerability to cyber-risks! Many law firms have yet to realise the full extent of their exposure to risk particularly in relation to their use of the Internet.

*Almost every website is now caught by the Electronic Commerce (EC Directive) Regulations 2002, which came into force on 21 August 2002. It is not generally realised that from 23 October 2002, Trading Standards authorities have had the power to enforce its provisions with an order carrying fines and imprisonment!*

## WHAT PROCEDURES ARE IN PLACE

to raise awareness of technology risks in: communications and data; 'hackers'; abuse of passwords; viruses; and disaster recovery?

## WHAT PROCEDURES ARE IN PLACE

to raise awareness of legal and regulatory risks in: domain name security; web site information, advertising, copyright and data management; confidentiality; online advice, contracting and transactions?

## WHAT PROCEDURES ARE IN PLACE

to raise awareness of operational risks in: staff behaviour; defamation; pornography; harassment; monitoring of employee activity in using e-mail, the Internet, the firm's website; and delivery of electronic legal services?

## WHAT POLICIES ARE IN PLACE

to identify and evaluate the exposure to these risks; to develop a risk control plan; and create and maintain a risk register?

## WHAT POLICIES ARE IN PLACE

to eliminate, reduce and/or manage these risks by: the appointment of a risk manager; the assignment of suitable personnel to address: the technology risks; the legal compliance risks; the operational issues; and ensure senior management 'buy-in'?

## DON'T DELAY – GET AUDITED TODAY!

The Web4Law audit consists of a day's visit to the firm to interview any partners and staff responsible for IT use and preparation of a report highlighting actions needed and provision of sample policies. Any further advice will be clearly proposed and costed for your consideration.

**Contact Web4Law's cyber-risk expert, Rupert Kendrick, on  
[rupert@web4law.biz](mailto:rupert@web4law.biz)**

**WEB4LAW**

# Lexcel – a more Competitive



Nigel McEwen

## **Nigel McEwen, Managing Partner of Tarlo Lyons, talks to Managing Risk Editor, Rupert Kendrick, about the implications of the Lexcel standard for his practice**

**Tarlo Lyons is a law firm that takes its management strategies very seriously. “We went for Investors in People in 1998/99 and were accredited for Lexcel in August 2003. We wanted to improve the quality of our service and make ourselves more competitive,” says managing partner, Nigel McEwen.**

The firm is difficult to classify in the legal marketplace. With 22 partners, 100 staff and one office you could not say it was particularly large, medium or small. “I’d regard us as a niche firm, but in several

areas,” he says. “We specialise in IT law, tax investigations and gaming law, as well as the traditional areas of property and litigation.”

The option to go for Lexcel was a decision arising from an unusual strategy – for law firms at least. “We decided to commission a live interview survey of our 15 top clients. We felt that simply requiring completion of a *pro forma* survey would not give us the depth of information we wanted. We didn’t feel clients would reply with the candour or the degree of disclosure we were after.

“The findings were that our services were not totally consistent. In some respects, it appeared we were over-stretched in terms of staff and workload. We thought it through and decided that Lexcel could provide a framework that would help to manage the firm’s activities.”

He is very precise about the objectives of the exercise – it was clearly not simply to float another badge on the firm’s notepad. “I think there were five key objectives that I identified when we agreed to embark on accreditation. First, we wanted a more considered service delivery across all departments, which we felt would develop cross-selling potential as all departments would be performing to the same standard.

“Second, we wanted a consistent approach to client communications, so that, for instance, there was uniform handling of Rule 15 and similar client communications.

“Third, we wanted a greater level of supervision, for instance, through file reviews.

“Fourth, we were concerned about insurance premiums as the market was beginning to harden and we felt we’d be better placed to negotiate with insurers.

“Fifth, we had already achieved liP accreditation and we felt that a further accreditation in the form of Lexcel would demonstrate our commitment to quality standards.”

I noticed that nowhere in the list had he mentioned risk management. “I think

consistency in quality is, in fact, risk management by another name. After all, they’re both about efficiency and good governance – effectively minimising the exposure of a practice to claims of one sort or another.

“We were experiencing sharp growth in new areas of work, particularly in the IT sector and clients are ever becoming more aware. But I have to say that in the latest round, our insurers were not prepared to make the allowance on the firm’s renewal that I’d hoped for”.

It has always seemed strange to me that law firms have not achieved Lexcel in greater numbers, particularly as it is a standard specifically devised to help their efficiency and competitiveness. Nigel McEwen has some definite views on this, arising, not least, from having driven his firm through the process.

“I’m sure there’s a real lack of awareness generally in the profession over what Lexcel is about. Many firms have not explored it and are not attuned to it as a strategy. Then there’s the perception that it’s intrusive and that partners’ performances will be placed under the spotlight.

“There are all sorts of excuses offered for what is really apathy – change of working habits; the risk arising for client confidentiality; and so on. But partners, in particular, choose not to realise that the standard is not designed to scrutinise their legal work, but is rather a check on how it’s administered.

*The option to go for Lexcel was a decision arising from an unusual strategy – for law firms at least. “We decided to commission a live interview survey of our 15 top clients. We felt that simply requiring completion of a pro forma survey would not give us the depth of information we wanted. We didn’t feel clients would reply with the candour or the degree of disclosure we were after”.*

# Foundation for Changes

"And there's another problem. Lawyers are very committed to their clients and equally committed to the law – but talk to them about administration and they say it just gets in the way. It puts boundaries on their independence.

"But there's the rub, because Lexcel is designed actually to help administration, once the systems are in place, because it provides a clear allocation of tasks and responsibilities that avoids the need to go through repeated fire-fighting exercises. The fee earners can concentrate on fee earning."

I wonder how he found the accreditation exercise in his firm. "I found that we needed commitment from the top, of course, but I also found equally valuable was the commitment from administrative

## tarlo lyons

staff. They found they could work much more efficiently. Between these two 'layers' I could funnel the rest through the process!"

I returned to the issue of professional indemnity insurers. Had Lexcel proved beneficial? "We thought it would, but at the moment, the insurers are looking more at claims records, claims culture and complaints. Like many others, I thought they would be the drivers, but I think they feel that Lexcel is more of a 'tick-box' exercise than changing the way risk is managed.

"It may be that this will have to be driven by the Law Society. I don't think I'd argue strongly against the idea of imposing a

condition relating to Lexcel accreditation on practising certificates. After all, legal aid firms have to sign up to Legal Services Commission contracts, which require management standards to be in place before they provide legally aided services. What's the difference?"

We end by discussing the benefits. "I think it goes to performance. It has made us much more competitive, in terms of our risk awareness and management. It also has certain benefits when tendering for work and it helps us plan our future strategy with greater precision.

"It gives us the foundation for a more competitive performance, which I think all law firms are going to need with the changes that are likely over the next few years." •

HSBC Insurance Brokers Limited  
Professional Indemnity Insurance services for Solicitors



- Risk Management Advice and Solutions
- Indemnity Review and Placement
- Exclusive Qualifying Insurer quote facility
- Claims Handling Service
- Lexcel Consultancy
- Personalised Client Care
- Practice Visits

Should you require our team to review your existing arrangements or just provide you with an alternative quotation, please do not hesitate to contact the Team.

Janine Parker – Assistant Director – 0207 661 2373  
William Cooper – Senior Professional Indemnity Executive – 0207 661 2312  
Helen Mortonson – Professional Indemnity Executive – 0207 661 2089  
Rachel Rowlands – Claims Director – 0207 661 2047

## Managing Audit and Compliance Visits

### *Ian Austin LLB, LLM, Practice Development Consultant, explains how law firms should approach and manage audit and compliance inspections*

**Professional Standards Unit (PSU) visits – effectively audits, by any other name – have now become a fact of professional life, with the recent recruitment of a full complement of Investigating Officers to the Unit, in pursuance of the Law Society's declared policy of effecting visits to all firms every three years, irrespective of whether a firm is subject to a complaint or there are specific identified issues of professional concern.**

Originally geared to promoting compliance with the Solicitors Costs Information and Client Care Code 1999, visits now embrace a wider range of regulatory issues, including the internal operation of money-laundering procedures, and can be undertaken on a random basis, although client complaints, particularly of a persistent nature, will continue to take priority.

#### **Wide-ranging nature**

Although the Code has been operative for several years, there appears to be an extraordinary failure, in some quarters, to acknowledge its mandatory nature and, in general, to appreciate its detailed requirements and their impact upon the solicitor/client relationship.

The comparatively wide-ranging nature and complexity of these requirements include: more thorough coverage of costs information, the basis of charging in non-fixed fee cases, examination of alternative methods of funding instructions, written confirmation of the details of clients' instructions, regular costs updates, progress reports, costs benefit and risk analysis, and written notifications during the care and conduct of the matter, and

seems to have taken practitioners by surprise. There are few firms who can confidently proclaim to be compliant with the Code in every respect.

#### **Style of visits**

Although the style of most visits is intended to be consultative and to assist those practices who have not chosen to embrace LEXCEL Practice Management Standards (PMS) to attain a higher standard of professional relations with clients, to the benefit of the recipient firm and the profession in general, this should not obscure the regulatory nature of the process or the consequences of an adverse report.

The scope and investigative nature of the visit will markedly depend upon whether it is random, or triggered by specific professional concerns, which, in many instances, will not be disclosed or sourced to the firm prior to the visit.

In any event, it is clear that the style of PSU visits has evolved considerably since the Unit was founded. Typically, visits will now last two to three days, may involve more than one investigating officer, and are far more intensive than was previously the case.

#### **Findings**

All visits result in a written report which, depending upon its findings, will require a constructive response from the firm and specific commitments to corrective action in respect of any non-compliance with the Code or related regulations, even if they have only resulted in non-material breaches.

This is an important development in the client standards regime. Under the Code, a serious breach or persistent material breaches of its requirements would result in a breach of PR 15 and, potentially, an appearance before the Disciplinary Tribunal. Additionally, such breaches might be evidence of inadequate professional services under section 37A of the **Solicitors Act 1974**. Single instances of material breach could, of themselves, lead to infringement of section 37A, with the possibility of disallowance of part or all of the firm's costs and/or a direction to pay compensation to the client of up to

£5,000. Non-material breaches were not specifically dealt with under the Code.

*The scope and investigative nature of the visit will markedly depend upon whether it is random, or triggered by specific professional concerns, which, in many instances, will not be disclosed or sourced to the firm prior to the visit.*

#### **Retainers**

Of most frequent concern, ironically, are the contractual relations under which many firms accept client's instructions. While it is true to say that virtually all firms now have and actively utilise standard terms of retainer, a great majority of these are defective in respect of several of the Code's requirements, and are frequently unsuited to the full range of instructions that are accepted by a practice.

Probate, for instance, requires the application of radically different terms and conditions to contentious work. This appears to be equally true of those firms accredited under Lexcel PMS, which would seem to suggest that auditing processes under the current accreditation scheme fail to concentrate sufficiently on the detail and practice of client care procedures operating within firms.

#### **Criticisms**

One of the main criticisms made by accredited firms concerns the apparent lack of practical legal experience of some auditors, which may go some way to explaining this.

In contrast to some of the quality accreditation bodies and, it must be said, the Legal Services Commission, the PSU has, in a protracted and appropriately solicitous recruitment campaign, gone the proverbial extra mile to ensure that people of the necessary calibre and experience are recruited as Investigating Officers.

Hopefully, Lexcel PMS accreditation may, in future, fall within the remit of a properly resourced PSU, although this would likely overburden the Unit in the immediate term. •

# Tipping Off – What can we tell the Clients?

*Matthew Moore identifies legal and professional risk issues that arise when considering whether to inform a client of a report under the Proceeds of Crime Act 2002*

**When the Proceeds of Crime Act 2002 ('the Act') took effect last year, there were widespread fears of liability for the offence of 'tipping-off'. Many firms took the view that even to do so much as to warn their clients about the reporting regime could, in effect, constitute the offence.**

A closer examination of the provisions shows how this could never have been the case, but the reaction of many delegates on our combating money laundering training sessions shows that such concerns still remain.

## The law

Section 333 of the Act provides that:

A person commits an offence if – (a) he knows or suspects that a disclosure within section 337 or 338 has been made, and (b) he makes a disclosure which is likely to prejudice any investigation which might be conducted following the disclosure referred to in paragraph (a).

Leaving aside the obvious criticism of the drafting, with the unfortunate repetition of the word 'disclosure' to cover both reports to the authorities and then also in paragraph(b) in relation to what is communicated to the client, it is clear that this offence can only be committed when a disclosure to the authorities has arisen under the Act.

On the important issue of timing, it should be noted that both disclosures are made in accordance with an employer's procedures, so a representative of the firm would seem to be at risk from the point where an internal report to the

Reporting Officer (MLRO) is made and not from the later stage where a disclosure is made externally.

If no disclosure has yet been made, what then is the risk? An offence easily overlooked, as it is outside section 7 of the Act, is section 342 which is headed 'Prejudicing an Investigation'. This provides that:

"(1) This section applies if a person knows or suspects that an appropriate officer... is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation or a money laundering investigation which is being or is about to be conducted.

"(2) The person commits an offence if (a) he makes a disclosure which is likely to prejudice the investigation, or (b) he falsifies, conceals, destroys or otherwise disposes of or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation."

The first part of this offence is clearly the greater concern for professional advisers but, again, the offence is limited in when it can be committed. The adviser in a law firm must 'know or suspect that an officer is acting or is proposing to act', which would seem unlikely when the circumstances behind a potential report first come to light.

## Taking instructions

When first taking instructions, therefore, with no disclosure yet made and no prospect of an investigation having been started or planned, what risks do law firms' personnel face? The answer would seem to be limited to 'aiding and abetting' one of the principal offences of concealment, arrangement and acquisition use and possession (sections 327-329 of the Act). This would be a risk if the adviser were to stray into advising the client as to how they should suppress information to avoid later money laundering charges. This might sound unlikely, but the situation where the client wants advice on their liability might be seen to take the adviser uncomfortably close to this position. The Law Society also provides fairly bullish advice that,



Matthew Moore

notwithstanding the offence of 'Prejudicing an Investigation', the client should be entitled to seek advice on their legal position in relation to money laundering investigations. Section 4.74 of the Law Society guidance provides that:

"...if a client is aware that his bank has been in contact with the police, he is entitled to seek advice on his legal position and his legal adviser is entitled to advise him that he may be the subject of a money laundering investigation without the risk of being prosecuted for either offence, even if as a result such advice might prejudice an investigation."

If ever a detailed attendance note were vital, surely this is it!

## Privilege defence

The existence of legal professional privilege as a defence to sections 333 and 342 is a further complicating twist to the picture. Both sections entitle a 'professional legal adviser' to make disclosures to the client that would otherwise be an offence as long as there is no 'intention of furthering a criminal purpose'. Whereas the accountant or bank manager may say nothing, it would seem, once a disclosure has been made or an investigation is pending, the legal adviser can clearly do so.

This point was one of the central issues in the leading case of *P v P 2003 (EWHC 2260: Fam)*. The National Criminal Intelligence Service (NCIS) claimed that there could be no circumstances where an adviser advises on a disclosure since it would always have the effect of 'furthering a criminal purpose'. This was not accepted by Dame Butler-Sloss. The privilege defence would only break down where the adviser had an improper intention in providing the information. Thus, in *P v P*, the wife's solicitors would be entitled to reveal their disclosure to their client and to the solicitors representing the husband.

Does this give a general right to legal

continued on P12

continued from P11

advisers to tell their clients and opponents about disclosures or investigations? Not as matters stand. The actual legal position is complicated by the fact that there are different standards of privilege in the Act. Section 330, with its duty on those in the regulated sector to make disclosures, excuses situations where the information comes to an adviser 'in privileged circumstances' – thus specifically invoking the law of evidence on this complex point.

On the other hand, sections 333 and 342 merely permit the adviser to make disclosures to the client or others 'in connection with the giving by the adviser of legal advice to the client' or 'in connection with legal proceedings or contemplated proceedings' (sections 333:3 and 342:4). The best we currently have on this is the judgment in *P v P* which suggests that the adviser can inform the client or another of

a disclosure or investigation where 'necessary and appropriate' (para 65).

### Implications

What might this mean in practice? Before we have test case prosecutions or clearer guidance from the authorities we simply do not know, but it is possible that *P v P* will eventually be seen to be a case on family law first and foremost, with the judgment shaped by the duty of full and frank disclosure in ancillary work arising under case law.

This might mean that a family lawyer would be on firm ground in telling their client about a disclosure; and recent advice from the Solicitors Family Law Association and the Bar Council certainly support this view. On the other hand, it could be argued that it is neither 'necessary' or 'appropriate' for a conveyancer to inform a client that they had disclosed their suspicions about the source

of the funds in a transaction.

Firms are taking into account the Law Society's advice that simply because an adviser might be able to inform their client of disclosures they do not have to do so (see Law Society guidance: 4:71). In most cases, firms will choose not to tell their clients about disclosures and this is bound to be the safer course of action, not least because *P v P* as a family law case will not be binding on the criminal courts in any prosecution, even if it is strongly persuasive.

What is clear, however, is that blunt warnings to clients at the outset of instructions are not just permissible but also advisable if the firm is to avoid the later complications of disclosures and if the law is to achieve its stated main aim of preventing, rather than penalising, money laundering. •

WEB4LAW

## LEXCEL ADVICE from Web4Law

We have a team of expert consultants who can advise generally on the Lexcel programme or provide specific advice on particular elements. Our experience is that most firms have a manual which is largely compliant with the new standard but often need assistance to make the procedures a reality. We prefer to work with firms to help them develop the necessary system rather than impose a standard package. Firms wishing to obtain specific advice on elements of the new standard might like to consider:

### Structures and Policies

Advice on limited liability partnership conversions, strategic elements of quality management systems, provision of money laundering advice and training for compliance with the MLR 2003

### Strategy, the Provision of Services and Marketing

Business planning and marketing reviews – chairing of partnership weekends a specialisation

### Financial Management

Training on time capture and enhanced financial controls

### Facilities and IT

Fixed price computer use audit and report service

### People Management

Training in all elements of recruitment, appraisal and people management skills, advice on partner appraisals and reward schemes

### Supervision and Risk Management

Advice on the development of risk strategies and training in supervision – our experience being that partners and team leaders often fail to take their supervisory duties sufficiently seriously

### Client Care

Advice and training in all aspects of improving the services provided to clients

### Case and File Management

Advice on the development of appropriate systems and procedures and staff training to enhance awareness of the system – if this is a problem try our 'quality quiz'!

### LEXCEL CONVERSIONS WITH WEB4LAW

- Advice to management on what is entailed in a conversion
- Fixed price Information Risks audit and report
- Cross referencing and checking of current manuals

Contact Simon Bray (Lexcel Consultant) at [simon@web4law.biz](mailto:simon@web4law.biz)

WEB4LAW

# Is your Firm Data Protection Risk Free?

*Although lawyers are excellent at offering compliance advice to their clients, they can be slow to implement data protection procedures in their own working environment. Peter Carey, consultant solicitor to Charles Russell, considers the most common areas of non-compliance for law firms.*

**Perhaps it is because law firms are so heavily regulated that there is a measure of complacency when it comes to data protection compliance. In conducting data protection compliance reviews for law firms, the following areas often require some remedial attention.**

**The collection of client information**  
It is obvious that a law firm must comply with the usual data protection requirements in respect of client data – examples include using data only for the purposes for which those data are acquired, ensuring the security of data and destroying obsolete data.

The 'fair processing' obligations in the Data Protection Act 1998 ('DPA') additionally require that certain information must be supplied at the point of data collection: the identity of the business, the purposes for processing and 'any other information to enable the processing to be fair'.

The purposes for which a law firm collects client data include money laundering checks, the provision of legal advice and marketing. Individual clients should also

be informed of their right of 'subject access' under section 7 of the DPA. The most logical place to provide such information is the Rule 15 letter.

#### **The outsourcing of business functions**

Certain requirements arise out of the relationship that exists between the law firm and the organisations to whom it outsources data processing – examples include payroll companies, web site hosts and confidential waste management agents. Most, if not all, law firms use at least one outsourcing company in this way.

The DPA renders such outsourcing arrangements unlawful without certain formalities being present – first, the contract must be in writing; second, the contract must contain certain minimum obligations on the outsourcee, namely an obligation to process personal data only on the instructions of the law firm and to take security measures equivalent to those imposed in the law firm under the seventh data protection principle (see below).

#### **Direct marketing by e-mail**

The law on e-mail marketing changed on 11 December last year. By virtue of the Privacy & Electronic Communications (EC Directive) Regulations 2003, it is now, subject to one exception, unlawful to send marketing e-mails without having obtained prior opt-in consent.

The exception, where it is still possible to send marketing e-mails with opt-out consent, applies where the law firm obtained the electronic contact details directly from the intended recipient in the context of the sale of a product or service, it uses the details to market similar products and services and it gives an opt-out (or 'unsubscribe') facility in each and every electronic marketing communication.

Law firms should be aware that the mere sending of 'e-mail updates' to clients and prospective clients constitutes 'direct marketing' and is subject to the new restrictions. The most logical place to obtain consent for marketing is in the Rule 15 letter.

#### **Security**

The seventh data protection principle in the DPA requires UK businesses to take "appropriate technical and organisational measures" to ensure the security of the personal data that they process.

A survey conducted by a private detective agency in late 2002 showed that law firms are generally 'very poor' at implementing appropriate data security procedures.

Common breaches of the seventh principle include leaving files on desks after hours and leaving computers on standby.

Detective agencies apparently routinely gain access to law firms via the cleaning staff at night, and by putting 'temps' into the workplace.

#### **Registration**

It is a legal requirement of all businesses in the UK to register (or 'notify') with the UK data protection regulator – this can be done online at [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk).

Although there are some limited exemptions from the registration requirement, law firms are unable to benefit from the exemptions.

When registering, law firms must state the purposes for which they process personal data (there are 33 to choose from, one of which is 'processing for the purpose of providing legal services') and must indicate whether they transfer data outside the European Economic Area.

Using personal data in a business in a manner which is incompatible with the register entry is a criminal offence.

**Peter Carey is author of 'Data Protection – a practical guide to UK and EU law' and is running half-day data protection compliance courses for Legal Practice Managers in Manchester on Thursday 9 September and in London on Monday 25 October and Monday 20 December.** •

Further details at: [www.privacydataprotection.co.uk/training](http://www.privacydataprotection.co.uk/training)

# People – your biggest Asset or biggest Risk?

*Charlotte Points, Training Consultant on Personnel and HR Development issues, outlines some of the key risks and pitfalls of managing people in the office*

**Employing others has a huge potential for exposing any organisation to risk. If a recruitment process is wrong, we may run into claims of unfair treatment, particularly if we are asked to disclose reasons for rejecting certain candidates.**

If we are asked to provide a reference for an employee, are we aware of the potential consequences of providing a judgement as well as the facts? If we decide to restructure, resulting in redundancies, are the pitfalls clear?

### **Pitfalls for the unwary**

More often than not, we are looking to the business need, focusing on the immediate problem and looking for a solution. Unless managers happen to be practising employment lawyers, unseen pitfalls await the unsuspecting.

These situations may appear in any organisation; and there are others – whistle-blowing, working time, discrimination, equal pay... the list of current employment legislation keeps increasing, and age discrimination is looming. How does the manager – more often than not a practising professional with a full client portfolio, avoid these traps?

### **The psychological contract**

The answer lies in good human resource management practice and sound policies, by which organisations, however small, strive to be a fair and honest employer of people. These policies can be established to keep partners or other managers on track.

However, equally fundamental to the employee/employer relationship is the contract – not legally binding terms – but the psychological contract; the unspoken element that defines the basis of a good working relationship – the deal an employee expects above the basic transaction of ‘I will work for you and you will pay me’.

If managers can create a culture and environment which allows an employee to see the benefits of the working arrangements – whether in terms of career development or identification with the organisation – we create an environment which encourages cooperation and openness and, at least, allows discussion of



potential risk situations before they develop. Such employee relations can help an organisation avoid many risk situations.

### **Building a structure**

How do we start to build a strong culture of respect and honesty? Employers, too often, are perceived by employees as breaking their side of the contract. It is often in everyday interaction between management and staff – the request to stay late once too often without thanks; refusal to accommodate a training course; denial of promotion or the chance to work with a special client; or higher pay for a new recruit than an existing employed solicitor.

Some argue that you can have no psychological contract between an organisation and an individual. Others say that if it exists purely in the mind of an employee, it does not exist as a contract.

However, an employee’s level of motivation and commitment to an organisation is dependent on their views

on how fairly they judge themselves and others to be treated, and whether what they see and feel confirms or denies the truth of the psychological contract.

Recent years have seen a growth in the restructuring of firms. The arrangement of an employee offering loyalty and commitment in return for a job for life has changed. Employers need to be more imaginative. Redundancy is more prevalent and other changes bring a new flexibility and uncertainty into careers.

Some can cope with the new arrangements – working hard for high rewards, accepting there will be no continuity of employment. Given the current climate of cut-throat competition, it is unlikely we can carry on paying more for the skills we need and, in future, we may be courting, once again, the goodwill and loyalty of our employees.

They prefer to belong to, and work with, an organisation in return for some security. They are likely to feel a strong sense of injustice if they perceive unfairness and will show this by leaving, or, more likely, by starting to withdraw from the organisation – not participating in social activity, or not volunteering to help others. Such discontent can spread and the risk to the organisation of a haemorrhaging of staff, or rapidly worsening ‘employee’ relations can potentially lead to many claims for unfair treatment.

### **Basic rules**

How can an atmosphere of trust be created? Some basic rules can be observed:

- decide on your ethos – different firms have different views – clarify yours;
- communicate it through your policies and processes;
- walk it as well as talking it;
- gain feedback from those you employ, those you would like to employ and those who have left you, and act upon it;
- think fair and act fair;
- admit it if you get it wrong and do better next time.

This kind of risk management is about relationship building. Think of staff relationships as those with a client and move towards a long term arrangement. •

## Managing E-mail In The Office

Monica Seeley and Gerard Hargreaves;  
Butterworth Heinemann; 2003;  
Pbk; 220 pages;  
ISBN 0 7506 5698 0

This book sets out to help those who feel that e-mail is taking over their lives. Its objective is to provide practical help and guidance on how an employee can manage both his or her own e-mail load and that of the organisation. The book expresses the hope that the reader will 'find winning ways with e-mail and reclaim some of the valuable resources which e-mail consumes'.



The book offers solutions which are aimed at helping to save time and to use e-mail to communicate the right message, 'right first time'. They are based on personal preferred patterns of work and management styles. The authors explain how to use e-mail in ways that improve productivity and reduce stress. Case studies are included throughout, which can be mapped across an organisation for easier understanding.

Subjects addressed include: taking control of your in-box; what your in-box says about you; assessing your e-mail 'fitness'; auditing your in-box; using e-mail with a PA; communicating in the e-mail office; e-mail on the move (necessity or option?); the e-mail gender gap; technology to manage e-mail traffic; ways of creating e-mail best practice; and the in-box of the future.

This is a 'fun' look at e-mail but in a constructive and instructive way – a way that enables the reader to enjoy the subject rather than baulk at yet another publication on e-mail management. It is likely to prove of value at all executive and management levels in an organisation.

## Stealing The Network

Ryan Russell; Tim Mullen;  
Dan Kaminsky; Joe Grand; Ken Pfeil;  
Ido Durbrowsky; Mark Burnett and  
Paul Craig;  
Syngress Publishing Inc; 2003;  
UK: Elsevier Science Ltd;  
Pbk; 300 pages;  
ISBN 1 931836 87 6

This book is a complete departure from the traditional publications on Internet security. It is a hybrid of textbook and fiction. As the foreword states, it "is a unique book in the fiction department. It combines stories that are fictional with technology that is real." It explains that while none of the events specified in the in the various chapters has occurred, there is no reason why they should not do so. The book provides a glimpse into the creative minds of hackers.

The authors are responsible for one section each. They are well-qualified to write on the techniques employed by hackers. For instance, Dan Kaminsky is senior security consultant for Avaya's Enterprise Security Practice; Mark Burnett is an independent security consultant and specialist in securing Windows-based Web services; and the others are equally well versed in hacking strategies and tactics.



The book suggests that people do not really understand what motivates or what deters hackers. They are a menace yet so many people revere them and even hire them. They steal, but what they steal isn't something tangible like a wallet or a car – it's just a network. They steal the network!

There is a good deal of technical detail in some of the sections and, as an American publication, the book is written in an American style with jargon to match. Providing this does not prove a deterrent, the reader will find this an informative, instructive and even entertaining book.

## Data Protection Strategy

Richard Morgan and Ruth Boardman;  
Sweet & Maxwell; 2003;  
Pbk; 280 pages;  
ISBN 0 421 83830 2



The subject of data protection is proving to be a quagmire into which many organisations sink without any prospect of surfacing. The Court of Appeal has described it as a 'thicket'.

The net result is that it is regarded as 'too complicated' and is then either ignored, or applied over restrictively.

This book tries to take a fresh approach. It does not require the reader to master the full detail of the data protection legislation before considering the topic further. Rather, it provides the theory in a single short chapter and then expands into the consequences of non-compliance. This enables the reader to proceed, at a fairly early stage, with an audit of the organisation.

The key features of the book include: how to go about a data protection audit; setting up strategies, policies and procedures; notification under the **Data Protection Act 1998**; compliance with the eight data protection principles; exemptions and the extent of their application; handling e-mail in compliance with the Act; and a comprehensive list of actions arranged by corporate functions within the average company – the Board, human resources, IT and legal departments, marketing, etc. It includes the Information Commissioner's Employment Code Part 3, which gives guidance on monitoring.

One of the authors, Richard Morgan, is an IT consultant with almost 40 years' experience of IT and is a Fellow of the British Computer Society.

The result is that this is a book for which practicality is of the essence. It combines, legal, technological and managerial issues capably and with clarity. It is highly recommended.

## Conferences and Events

### Key risk management events

**19 June 2004**

**New Discrimination Regulations – meaning and compliance LexisNexis UK Conferences and Training, 020 7347 3573 – London**

This event focuses on: the general principles of the new legislation; race and sex discrimination; religious belief discrimination; rights and diversity policies; DDA obligations; identification and development of a strategy for age discrimination; and features some of the leading authorities in discrimination law.

**15-17 June 2004**

**Internet World. Register at [www.internetworld.co.uk](http://www.internetworld.co.uk) Earl's Court, London**

This event focuses on the current issues facing organisations developing web marketing and security strategies, with: case studies and white papers; the latest products and solutions; news reviews and opinions and dedicated areas for new media issues; security and payments; content management; and mobile and wireless technologies.

**24-25 June 2004**

**Sarbanes-Oxley – Compliance. MIS Training, 020 7779 8153 – London**

This event focuses on the corporate governance issues raised by this legislation and will help with compliance and address the critical nature of the risks it raises. Although USA legislation, there will be corresponding legislation shortly in the UK and the general principles are relevant and important to all large organisations.

**30 June 2004**

**Security and Surveillance in the Workplace, LexisNexis UK Conferences and Training, 020 7347 3573 – London**

This event examines: recruitment and contract issues; monitoring the use of telephones, Internet, and e-mail; employee records; keeping and maintaining lawful records and requests for disclosure; and security measures; and will be addressed by leading exponents in their respective fields.

**7 July 2004**

**Stress at Work 2004 LexisNexis UK Conferences and Training, 020 7347 3573 – London**

This event will revisit the effects of stress on both employers and employees, updating delegates on strategies of how to deal with stress in the working environment. Specific issues addressed will include: stress and pressure issues at work; recognition of stress in others and how to intervene; and changing the organisation's culture to become stress-free.

**7-8 July 2004**

**Risk Management Congress 2004 IIR Ltd., 020 7915 5055 – London**

This event comprises a suite of sessions under each of the following streams: enterprise risk management; risks facing organisations today; world class risk functions; business continuity; insuring risks; operational risk management; health and safety; and corporate governance.

**8-9 July 2004**

**Contemporary Issues in Global IT Law Society for Computers and Law, 0117 9237393 – Oxford**

This event focuses on all legal issues surrounding the use of IT in law firms, and includes subjects such as: international outsourcing; technology contracts; data protection; mobile commerce; and e-commerce, and is supported by a full calendar of social events throughout the weekend of the event.

**12 July 2004**

**Discrimination Law – Introduction LexisNexis – IRS Training 020 7347 3500 – London**

This event focuses on discrimination at work and the potential legal liability of your organisation. Discrimination can occur during recruitment, in the treatment of an employee, in dismissal, or even in the provision of a reference. This event explains how to develop and implement protection strategies.



**For further information, please contact:**

**Janine Parker —Assistant Director/Lexcel Consultant — 0207 661 2373**

**Helen Mortonson — Professional Indemnity Executive — 0207 661 2089**