

Cyber security for law firms

Chris Kirk-Blythe, CEO, LBS Legal



Free online training for you and all your staff

Access via Law Society learning

Cyber Essentials Scheme (government guidance)

The screenshot shows a web browser window with the URL <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>. The page is titled "Documents" and lists three PDF documents:

- [Cyber Essentials Scheme: Summary](#)
Ref: BIS/14/696
PDF, 499KB, 10 pages
- [Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks](#)
Ref: BIS/14/696
PDF, 501KB, 17 pages
- [Cyber Essentials Scheme: Assurance Framework](#)
Ref: BIS/15/72/
PDF, 546KB, 12 pages

At the bottom of the page, there is a "Detail" section with the text: "The government has worked with the Information Assurance for Small and...". The Windows taskbar is visible at the bottom, showing the search bar and various application icons. The system tray shows the time as 21:25 on 19/10/2015.

SRA publication

- Spiders in the web:
- The risks of online crime to legal business
- March 2014

Legal career 'hit by vishing scam'

By Joe Lynam and Ben Carter
BBC Radio 4's Money Box

2 October 2015 | Business



Karen Mackie says she is devastated about what happened

A solicitor has told the BBC that being tricked into transferring £750,000 of client money to criminals has left her life in ruins.

Sole practitioner Karen Mackie has been suspended from working, declared bankrupt, and faces the prospect of losing her home.

She is the latest victim of "vishing" in which criminals pose as bank security teams.

Karen Mackie

Where did she go wrong?

Top Stories

Chinese president in UK for state visit

Chinese President Xi Jinping arrives in the UK at the start of a four-day state visit which UK PM David Cameron has said marks a "golden era" in ties.

4 minutes ago

Parts of Caparo steel in administration

2 hours ago

Serial killer suspect 'drugged victims'

53 minutes ago

Features



'Sikh Lives Matter'

The protest movement that interrupted BBC programming



LBSLegal

SRA Update

- 50 firms have reported to the SRA that they have fallen victim to cyberattacks in 2015
- Criminals are finding ever-more sophisticated ways of targeting the legal sector
- The SRA has announced that the number of attempted thefts has continued to rise this year
- Thefts ranged from £40,000 and £2m
- The problem is only going to get worse and worse

The new jewellers

Why are cyber criminals targeting you?

Legal



The new bakers

why are criminals targeting you?

- ‘When it comes to cyber security, small English law firms have the infrastructure, the knowledge, and the sophistication of a local bakery store, but they control banking transactions exceeding, in value, the balance sheets of many medium-sized banks.
- This sector is a gift to the cyber criminal. Small law firms are soft targets with lots of money.
- To cyber criminals, small law firms represent the equivalent of walking into a local bakery with a water pistol and leaving with £500k and very little chance of getting nicked’
 - Paul Teller, National Fraud Intelligence Bureau March 2015

The Mandatory Principles

1. uphold the rule of law and the proper administration of justice;
2. act with integrity;
3. not allow your independence to be compromised;
4. act in the best interests of each client;
5. provide a proper standard of service to your clients;
6. behave in a way that maintains the trust the public places in you and in the provision of legal services;
7. comply with your legal and regulatory obligations and deal with your regulators and ombudsmen in an open, timely and co-operative manner;
8. run your business or carry out your role in the business effectively and in accordance with proper governance and sound financial and risk management principles;
9. run your business or carry out your role in the business in a way that encourages equality of opportunity and respect for diversity; and
10. protect client money and assets.

The Mandatory Principles

1. uphold the rule of law and the proper administration of justice;
 1. ‘...it is necessary in our society, a society in which the restraining and controlling framework is built upon a belief in the rule of law, that communications between clients and lawyers, whereby the clients are hoping for the assistance of the lawyers' legal skills in the management of their (the clients') affairs, should be secure against the possibility of any scrutiny from others, whether the police, the executive, business competitors, inquisitive busy-bodies or anyone else.’ Lord Scott of Foscote in *Three Rivers District Council and others v. Governor and Company of the Bank of England* [2004] UKHL 48
 2. ‘The principle which runs through all these cases, and the many other cases which were cited, is that a man must be able to consult his lawyer in confidence, since otherwise he might hold back half the truth. The client must be sure that what he tells his lawyer in confidence will never be revealed without his consent. Legal professional privilege is thus much more than an ordinary rule of evidence, limited in its application to the facts of a particular case. It is a fundamental condition on which the administration of justice as a whole rests.’ Lord Taylor of Gosforth in *R v Derby Magistrates Court ex p B* [1996] AC 487

The Mandatory Principles

1. uphold the rule of law and the proper administration of justice;
2. act with integrity;
3. not allow your independence to be compromised;
4. act in the best interests of each client;
5. provide a proper standard of service to your clients;
6. behave in a way that maintains the trust the public places in you and in the provision of legal services;
7. comply with your legal and regulatory obligations and deal with your regulators and ombudsmen in an open, timely and co-operative manner;
8. run your business or carry out your role in the business effectively and in accordance with proper governance and sound financial and risk management principles;
9. run your business or carry out your role in the business in a way that encourages equality of opportunity and respect for diversity; and
10. protect client money and assets.

Mandatory Outcomes & Indicative Behaviours

- **Chapter 7: Management of your business**
 - O (7.5) you comply with legislation applicable to your business, including anti-money laundering and data protection legislation;
 - IB (7.1) safekeeping of documents and assets entrusted to the firm;
 - IB (7.3) identifying and monitoring... operational risks including claims under legislation relating to matters such as data protection, IT failures and abuses...;

Confidentiality & Disclosure

- O (4.1) you keep the affairs of clients confidential unless disclosure is required or permitted by law or the client consents;
- O (4.3) you ensure that where your duty of confidentiality to one client comes into conflict with your duty of disclosure to another client, your duty of confidentiality takes precedence;
- O (4.5) you have effective systems and controls in place to enable you to identify risks to client confidentiality and to mitigate those risks.
- IB (4.1) your systems and controls for identifying risks to client confidentiality are appropriate to the size and complexity of the firm and the nature of the work undertaken, and enable you to assess all the relevant circumstances;
- IB (4.2) you comply with the law in respect of your fiduciary duties in relation to confidentiality;
- IB (4.3) you only outsource services when you are satisfied that the provider has taken all appropriate steps to ensure that your clients' confidential information will be protected;
- IB (4.5) not acting for A where B is a client for whom you hold confidential information which is material to A unless the confidential information can be protected.
- IB (4.6) not disclosing the content of a will on the death of a client unless consent has been provided by the personal representatives for the content to be released;
- IB (4.7) not disclosing details of bills sent to clients to third parties, such as debt factoring companies in relation to the collection of book debts, unless the client has consented.

Fiduciary Duties to clients

- A fiduciary is someone who has undertaken to act for or on behalf of another in a particular matter in circumstances which give rise to a relationship of trust and confidence. The distinguishing obligation of a fiduciary is the obligation of loyalty. The principal is entitled to the single minded loyalty of his fiduciary. This core liability has several facets. A fiduciary must act in good faith; he must not make a profit out of his trust; he must not place himself in a position where his duty and his interest may conflict; he may not act for his own benefit or the benefit of a third person without the informed consent of his principal.
- *Bristol & West Building Society v Mothew [1998]*.

SRA Authorisation Rules 2011

- Rule 8 imposes some general conditions upon your firm's SRA authorisation, including that you:
 - comply with SRA rules and with statutory obligations (including DPA 1998);
 - have suitable arrangements for compliance with SRA rules and with statutory obligations (including DPA 1998);
 - Maintain the professional principles (s.1(3) Legal Services Act 2007) which include 'that the affairs of clients should be kept confidential';
- If you fail to abide by these general conditions Rule 22 allows the SRA to revoke or suspend your firm's authorisation, which means you have to close your practice.

Legal Ombudsman

- Despite the regulatory powers of the SRA and the Information Commissioner, the Legal Ombudsman (LeO) still can – and does – deal with data-related complaints.
- Last year LeO took slightly over 80 (about 1 percent) complaints about data protection/breach of confidentiality, and upheld 8 of those.
- LeO can award compensation to clients of up to £50,000.00 plus interest and charge you £400 for each complaint;
- LeO may refer the complaint to the Information Commissioner and / or the SRA;

So just one data leak may, theoretically at least, result in...

- A professional negligence claim for breach of fiduciary duty;
- A complaint to the Legal Ombudsman;
- Disciplinary action by the Solicitors Regulation Authority;
- Prosecution before the Solicitors Disciplinary Tribunal;
- Revocation or suspension of the firm's SRA authorisation;
- Regulatory action by the Information Commissioners Office;
- Criminal prosecution in the Magistrates or Crown Court;
- Disciplinary action by your employer for gross misconduct;
- Civil action against you personally for breach of employment contract, duty of care etc.

Common mistakes

- Password sharing
- Unlocked PCs
- iPads, iPhones etc
- Laptops
- Emails
- Trains and coffee shops

The biggest problem is still

LBSLegal

PEOPLE

- Your employees are irrepressible
- Your employees are unpredictable
- Your employees are inconsistent
- Your employees are disobedient
- Your employees are unmanageable
- Your employees are uncontrollable
- Your employees are temperamental