

available at [www.sciencedirect.com](http://www.sciencedirect.com)[www.compseconline.com/publications/prodclaw.htm](http://www.compseconline.com/publications/prodclaw.htm)


---



---

**Computer Law  
&  
Security Report**


---



---

## IT security

# Legal developments in IT security<sup>☆</sup>

**Mike Conradi\***

Kemp Little LLP, London

---

### A B S T R A C T

This article is based on a talk given by the author in May 2007 discussing the legal aspects of IT security. After first going through security-specific regulation applicable to all industries it describes in some detail relevant regulations applicable specifically to the financial services and communications' industries and explores the practical implications of these regulations for in-house lawyers and those advising them. The second part of the article discusses security-related provisions which should be considered for inclusion in any IT services contract.

© 2007 Kemp Little LLP. Published by Elsevier Ltd. All rights reserved.

---



---

## 1. "Party invitation of a lifetime!"

In January 2007, the NCC Group published the results of a study they had conducted into IT security.<sup>1</sup> They had sent a gift-wrapped USB memory stick to the Finance Directors of 500 UK public companies wrapped in packaging suggesting that its contents contained an exclusive "party invitation of a lifetime". More than half of the Finance Directors plugged in the USB stick and even clicked on the "Yes I want to install some software" option. The NCC's comment on this was:

*This demonstrates that a fundamental lack of a healthy suspicion by IT users remains even at a senior level. The need for real security awareness has never been greater. This is a serious issue amongst today's businesses and is something that everyone should have in the forefront of their minds.*

The study, and others like it, demonstrate that there is still some way to go, even amongst senior professionals, to raise awareness of possible IT security issues.

Also in January 2007, the UK's Serious Organised Crime Agency ("SOCA") took over the operations of the National Hi-Tech Crime Unit. They published a threat assessment<sup>2</sup> describing some of the serious IT security risks which they saw businesses and individuals facing. In particular, the threat assessment states that:

*Organised criminals are using a variety of hi-tech methods. These include:*

- *hacking into customer databases;*
- *infecting personal computers with malicious software to steal personal information for credit card and online banking fraud; and*
- *use of anonymised email accounts, data encryption and proxy computers, to evade detection.*

The threat assessment also noted that malware (that is software installed on computers for malicious purposes without the knowledge of the user) is becoming increasingly

---

<sup>☆</sup> This article is based on a talk given by Mike Conradi at Kemp Little's "Corporate Counsel Forum" on 25 April 2007.

\* Tel.: +44 20 7710 1640.

E-mail address: [mike.conradi@kemplittle.com](mailto:mike.conradi@kemplittle.com)

<sup>1</sup> <http://www.nccgroup.com/news/view-in-the-press.aspx?id=146>.

<sup>2</sup> [http://www.soca.gov.uk/assessPublications/downloads/threat\\_assess\\_unclass\\_250706.pdf](http://www.soca.gov.uk/assessPublications/downloads/threat_assess_unclass_250706.pdf).

0267-3649/\$ – see front matter © 2007 Kemp Little LLP. Published by Elsevier Ltd. All rights reserved.

doi:10.1016/j.clsr.2007.05.005

sophisticated, and noted that “Phishing” messages, which attempt to deceive the reader into thinking that they are from another party in order to obtain personal data, are becoming increasingly harder to distinguish from genuine ones, especially where the criminals use personal data they have obtained through other means in order to personalise them.

There are, then, a great deal of IT security threats which individuals and businesses face. The purpose of this article is to describe the law and the specific regulation in relation to IT security threats and then to discuss how, in practice, businesses might deal with some of these in their contracts with IT suppliers.

## 2. Law and regulation

### 2.1. Regulations applicable across all sectors

The starting point when discussing the regulation of IT security issues is the Combined Code on Corporate Governance, as published by the Financial Reporting Council in June 2006.<sup>3</sup> The Combined Code applies to any listed company in the UK and it contains an obligation, at “Main Principle” C.2 on a company’s board to “maintain a sound system of internal controls to safeguard shareholders’ investment and the company’s assets”. The Code continues, at C.2.1 that an annual review of those controls should be conducted and a report on their effectiveness should be produced. This review should “cover all material controls, including financial, operational and compliance controls and risk management systems”. This obligation would, clearly, cover an IT security system.

Similarly, under Section 404 of Sarbanes–Oxley,<sup>4</sup> US public companies must themselves maintain “an adequate control structure” and must ensure effective financial reporting procedures. Recognising that IT controls and security are vital for compliance with this obligation, the Act continues that there should be an annual audited assessment of the effectiveness of these internal controls and of the financial reporting procedures. US public companies, too, then, must also ensure they have an appropriate IT security system.

Turning back to the UK, the Data Protection Act 1998<sup>5</sup> imposes IT security obligations in respect of any personal data. The seventh Data Protection Principle states that “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data”. The Act continues that the IT security measures that must be taken should have regard to the technology available and to the cost of implementation and should be appropriate given the harm that might result from unauthorised or unlawful processing and given the nature of the data to be protected. It requires a data controller to take reasonable steps to ensure the reliability of any employees who have access to the personal data and states and that they should choose a processor

who provides sufficient IT security guarantees and then take reasonable steps to ensure that the processor complies with those guarantees.

The Act imposes further specific requirements in relation to the use of a data processor. It says that where a data processor is used, a data controller is not to be regarded as complying with the Seventh Data Protection Principle unless:

- (a) the processing is carried out under a contract;
  - which is made or evidenced in writing, and
  - under which the data processor is to act only on instructions from the data controller; and
- (b) the contract requires the data processor to comply with obligations equivalent to those imposed on the data controller.

The fact that the Data Protection Act contains this specific requirement is sometimes overlooked – either because a customer does not realise that the service it is receiving constitutes use by it of a data processor or because the specific requirements (and in particular the one which requires a processor to act only on instructions from a data controller) are otherwise overlooked. Unless these requirements are complied with, the data controller will be in breach of its obligations under the Act.

### 2.2. Sector specific rules

There are IT security-specific regulations applicable to many different sectors. For example the Aviation Security (Air Cargo Agents) Regulations 1993<sup>6</sup> and the Nuclear Industries Security Regulations 2003<sup>7</sup> both impose specific requirements in respect of their own sectors. This article, though, will concentrate on the two sectors which are likely to be most relevant to readers – financial services and electronic communications.

### 2.3. Financial services

The sector specific regulation for the financial services sector is published by the Financial Services Authority (“FSA”). The relevant rules are contained in the FSA’s “Handbook”<sup>8</sup> which is divided into several sections. The most relevant to this topic is the section known as SYSC (Senior Management Arrangements, Systems and Controls).<sup>9</sup>

SYSC 3.1<sup>10</sup> contains a rule that: “a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business”.

The Handbook continues with guidance which states that the nature and extent of the systems and controls will depend on a variety of factors including:

- the nature, scale and complexity of the business;
- the diversity of operations, including geographical diversity;
- the volume and size of transactions; and
- the degree of risk associated with each area of operation.

<sup>3</sup> <http://www.frc.org.uk/documents/pagemanager/frc/Combined%20Code%20June%202006.pdf>.

<sup>4</sup> [http://www.sarbanes-oxley.com/displaysection.php?level=2&pub\\_id=Sarbanes-Oxley&chap\\_id=PCAOB4&message\\_id=28](http://www.sarbanes-oxley.com/displaysection.php?level=2&pub_id=Sarbanes-Oxley&chap_id=PCAOB4&message_id=28).

<sup>5</sup> <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>.

<sup>6</sup> [http://www.opsi.gov.uk/si/si1993/Uksi\\_19931073\\_en\\_1.htm](http://www.opsi.gov.uk/si/si1993/Uksi_19931073_en_1.htm).

<sup>7</sup> <http://www.opsi.gov.uk/SI/si2003/20030403.htm>.

<sup>8</sup> <http://fsahandbook.info/FSA/html/handbook/>.

<sup>9</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC>.

<sup>10</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC/3/1>.

The guidance continues that a firm should carry out a regular review to ensure that it is complying with the obligation at SYSC 3.1.

There are further relevant obligations contained in SYSC. SYSC 4.1,<sup>11</sup> for example (which applies only to banks and institutions which trade securities (i.e. not to insurers)) requires that firms should, amongst other things, have “*robust governance arrangements, which include ... effective processes to identify, manage, monitor and report the risks it is or might be exposed to ... and effective control and safeguard arrangements for information processing systems*”. In respect of insurance companies, SYSC 13<sup>12</sup> contains some quite detailed requirements. SYSC 13.7.6<sup>13</sup> states that an insurer should “*establish and maintain appropriate systems and controls for the management and of its IT system risks*”. SYSC 13.7.7<sup>14</sup> states that an insurer should “*establish and maintain appropriate systems and controls to manage [its] information security risks*”. It continues that in doing so, a firm should have regard to:

- *confidentiality*: (i.e. information should be accessible only to persons with appropriate authority);
- *integrity*: (i.e. safeguarding the accuracy and completeness of information);
- *availability and authentication*: (i.e. ensuring access to information when required and by persons whose identity is verified); and
- *non-repudiation and accountability*: (i.e. ensuring that the person that processed information cannot deny their actions).

Finally, it is also worth noting that there are various places in the FSA’s Handbook which require a regulated entity to notify the FSA when they plan to outsource any critical or important function to a third party.

## 2.4. Communications

Article 4 of the Directive on Privacy and Electronic Communications (2002/58/EC)<sup>15</sup> imposes a specific IT security obligation on providers of publicly available electronic communications services (which basically means Internet service providers and telecoms operators). It states that they must “*take appropriate technical and organisational measures*” to safeguard the security of their services. They must also inform subscribers of particular security risks that they face and of appropriate measures they can take to safeguard themselves against the risk. This has been implemented in the UK by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) at Regulation 5.<sup>16</sup>

It is also worth mentioning that the European Commission is currently considering making a significant change in this area. The Commission’s proposals for modifications to Communications regulation, published as part of its “2006 Review”

in June 2006<sup>17</sup> suggested a modification which would oblige providers of electronic communication services to notify the relevant national regulator of any breach of security that led to the loss of personal data or to interruptions in the continuity of service supply. The regulator would then be able to inform the general public if it considered it to be in the public interest to do so. The Commission also suggested that providers should have an obligation to inform their customers of any such security breach.

If these proposals are implemented, this would be a significant change to the current rules in the communications sector as regards IT security. Similar (though broader) laws in the USA (and especially in California) have led to quite significant, and potentially embarrassing, disclosures. Under this law (The California Security Breach Notification Law, SB 1386<sup>18</sup>) Citigroup, for example, was forced to disclose that it had lost personal data, including names, social security details and account history on almost 4 million customers while storage tapes were in transit with UPS.

## 2.5. Security-specific standards

SYSC 13.7.8<sup>19</sup> requires that firms should “*ensure the adequacy of [their] systems and controls used to protect the processing and security of information, and should have regard to established security standards such as ISO 17799 (Information Security Management)*”.

Although this is only an obligation in respect of insurers, standards like the one referred to above are commonly used in IT contracts and it would be sensible for a customer in any sector to consider requiring their service providers to comply. The most relevant standards are ISO 17799, which is a code of practice on information security management and ISO 27001, which is a standard specification for an information security management system (“ISMS”). An ISMS is a means by which senior management monitor and control their security, minimising the residual business risk and ensuring that security continues to fulfil corporate customer and legal requirements.

## 3. Practical implications

In practice, it is important to realise that there is no legal obligation to *prevent* security breaches or data theft. Instead, the obligations are to have “*systems, controls or measures*” in place. For example, in February 2007, the FSA fined Nationwide £1 million after a laptop containing confidential customer data was stolen from an employee’s home.<sup>20</sup> The reason for the fine was not the theft itself, but because the theft revealed that Nationwide had failed to put in place

<sup>11</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC/4/1>.

<sup>12</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC/13>.

<sup>13</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC/13/7>.

<sup>14</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC/13/7>.

<sup>15</sup> [http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/L\\_201/L\\_20120020731en00370047.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/L_201/L_20120020731en00370047.pdf).

<sup>16</sup> <http://www.opsi.gov.uk/si/si2003/20032426.htm>.

<sup>17</sup> [http://ec.europa.eu/information\\_society/policy/ecommm/doc/info\\_centre/communic\\_reports/review/po\\_com\\_2006\\_334\\_reexam\\_ecomm\\_en\\_acte1\\_clean.pdf](http://ec.europa.eu/information_society/policy/ecommm/doc/info_centre/communic_reports/review/po_com_2006_334_reexam_ecomm_en_acte1_clean.pdf).

<sup>18</sup> [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html).

<sup>19</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC/13/7>.

<sup>20</sup> <http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml>.

“effective systems and controls” and had failed to have an adequate staff training programme.

Although the obligation does not extend to outcomes but only to having systems in place, it is pervasive – systems and controls must be “appropriate”, “adequate” and “sound”. Moreover, an assessment of compliance will often be made *ex post facto* – that is after there has been some specific breach. This means that there is a need for good record keeping so as to monitor the processes themselves as well as the IT systems. It also means that it is difficult to apply the standards and requirements in practice with any certainty as to whether or not enough is being done.

In practice, therefore, compliance can only be ensured by looking both internally and externally. Internally, in-house lawyers should examine the policies and standards which apply within their organisation. Externally, it is important for businesses to maintain contact and relationships with the relevant regulators and to ensure that contracts with third party suppliers contain appropriate provisions. This last point is discussed in the next section.

---

## 4. What contracts should contain

There are a number of provisions which it would be sensible to consider including in any contract with an IT security provider.

### 4.1. General IT security obligations

Under this heading, it would be sensible to consider obliging a supplier to comply with the customer’s security policies, to comply with applicable legislation and regulatory requirements relating to the secure operation and use of IT systems and, importantly, to comply with relevant industry standards such as ISO 17799.

It may also be sensible to add a requirement to comply with “Best Industry Practice” – a term which will need to be defined with reference to the practice of other suppliers in the same sector. In this context, it would probably oblige a supplier to ensure, for example, that it updates its software regularly, and that it maintains appropriate anti-virus and access control software.

### 4.2. Personnel

Where relevant, it would be sensible to include specific requirements on the supplier to carry out background checks on their personnel and to ensure that their personnel comply with the customer’s relevant policies and procedures. A customer may want the right to approve or reject individual personnel and to conduct their own checks. Importantly, there should be regular staff and supplier training on IT security issues (it was a failure to do this which led in part to the PSA’s Nationwide fine mentioned above).

### 4.3. Confidentiality

In the confidentiality section of the contract, suppliers should be obliged to protect the confidentiality of customers’

information and to prevent unauthorised access to the systems on which they are held. They should ensure that all confidential material is subject to appropriate access controls and that, for example, passwords are not shared between individuals. One area which is often overlooked is a requirement on a supplier to return or to delete copies of any confidential information in their possession on termination of the contract.

### 4.4. Data protection

In respect of data protection, it will be very important, if the supplier is processing personal data for the customer, to ensure compliance with the seventh Data Protection Principle discussed above. This means a clear obligation on the supplier only to process in accordance with the customer’s instructions and it may be sensible, also, to consider inserting a specific warranty linked to the seventh principle.

### 4.5. Reporting and audit

Where appropriate, the customer should expect detailed reports of all security incidents and periodic (for example monthly) reports covering issues such as unauthorised attempts to access the systems, virus incidents, outages or theft of any equipment. A customer should also have the right to audit a supplier’s compliance with its obligations – either itself or else by appointing a third party to do so.

The contract management procedure should include a continuous review and update on security issues and regular monitoring of compliance.

### 4.6. Liability

Although it is common in IT security contracts for a supplier to exclude all of its liability for indirect or consequential loss, there is always some uncertainty as to what this means in any given situation. If IT security is likely to be a particular issue, one thing for a customer to consider would be to introduce a specific term stating that irrespective of the exclusion of liability for consequential loss, a supplier will in fact be liable for “the cost of restoring lost or damaged data”. It is usually much easier for a supplier to agree to this specific carve-out than it would be for the supplier to agree to remove its exclusion of liability for consequential loss more generally.

### 4.7. Other matters

Other things to consider including in the contract include an obligation on the supplier to have a detailed disaster recovery and continuity procedure in place with regular back-ups and regular testing. If this is especially important, then details of the DR plan might even be attached as a schedule. Also, IT security should be treated as an important part of managing a disengagement on exit from the contract and we would normally expect to see items relating to IT security forming part of any exit plan.

---

## 5. Summary

As IT becomes an increasingly important part of just about any business, and as regulators seem likely to focus increasingly on IT systems as a component of managing risk, businesses should pay careful attention to ensure that their IT security systems are robust and up to date.

The aim of this article has been to describe the regulatory requirements that apply and to suggest briefly some sensible provisions to insert in contracts in order to assist with this.

**Mike Conradi** ([mike.conradi@kemplittle.com](mailto:mike.conradi@kemplittle.com)) Commercial Associate, Kemp Little LLP, London.